VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ

DEPARTMENT OF TELECOMMUNICATIONS

KVANTITATIVNÍ PŘÍSTUP K RIZIKOVÉ ANALÝZE V RÁMCI KYBERNETICKÉ BEZPEČNOSTI

QUANTIFIED APPROACH TO RISK ANALYSIS IN CASE OF CYBER SECURITY

BAKALÁŘSKÁ PRÁCE

BACHELOR THESIS

AUTOR PRÁCE — Petr Řezáč

AUTHOR

VEDOUCÍ PRÁCE — Ing. Radek Fujdiak, Ph.D.

SUPERVISOR

BRNO 2019

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní obor **Informační bezpečnost**
Ústav telekomunikací

Student: Petr Řezáč ***ID:*** 195165
Ročník: 3 ***Akademický rok:*** 2018/19

NÁZEV TÉMATU:

Kvantitativní přístup k rizikové analýze v rámci kybernetické bezpečnosti

POKYNY PRO VYPRACOVÁNÍ:

Student provede analýzu současného stavu problematiky jednotlivých přístupů pro hodnocení kybernetické bezpečnosti (kvalitativní, semi-kvantitativní, a kvantitativní). Hlavní zaměření a popis pak bude směřovat do kvantitativních metod a vyčíslení rizika, tedy i pravděpodobnosti jeho vzniku (pravděpodobnostní model – ovlivnitelné i neovlivnitelné faktory) a šíře jeho dopadu (aktiva, ekonomický faktor, lidské ztráty či zranění, aj.). Na základě teoretických poznatků, standardů a dostupné literatury bude vytvořena metodika pro kvantitativní hodnocení kybernetické bezpečnosti. Budou vybrány min. dvě specifické aplikace (doporučeno je vybrání např. infuzní pumpy a industriálního systému), které budou sloužit k demonstraci vytvořené metodiky. Výstupem práce bude softwarový nástroj pro realizaci dané metodiky a jejích dílčích částí (sestavení pravděpodobnostního modelu, výpočet rizika, atd.) sloužících pro kvantitativní kybernetickou rizikovou analýzu.

DOPORUČENÁ LITERATURA:

[1] HUBBARD, Douglas W a Richard SEIERSEN. How to measure anything in cybersecurity risk. Hoboken: Wiley, 2016.

[2] STONEBURNER, Gary; GOGUEN, Alice Y. a FERINGA, Alexis. SP 800-30: Risk management guide for information technology systems. 2002.

Termín zadání: 1.2.2019 ***Termín odevzdání:*** 27.5.2019

Vedoucí práce: Ing. Radek Fujdiak, Ph.D.
Konzultant:

prof. Ing. Jiří Mišurec, CSc.
předseda oborové rady

Abstrakt

Tato bakalářská práce se věnuje kvantitativnímu přístupu k rizikové analýze v rámci kybernetické bezpečnosti.

První část je věnována teoretické rovině. Jsou zde definovány základní pojmy spojené s problematikou kybernetické bezpečnosti a kybernetického prostoru. Je popsán proces řízení rizik dle normy ISO/IEC 27005 a podle metodiky NIST. Dále je provedeno srovnání jednotlivých metod rizikové analýzy. Závěrem jsou uvedeny příklady kvantitativních metod a představena triáda CIA.

Druhá část této práce je věnována vypracování QRA metody. Tato metoda je aplikována na dvě zařízení s výpočtem pravděpodobnosti, dopadu a míry rizika. Závěrem je provedeno vyhodnocení a srovnání obou zařízení.

Přínosem této bakalářské práce je sestavená metodika, která je uplatnitelná nejen pro stanovení samotného rizika, ale také lze podle ní porovnat jednotlivé systémy, zařízení nebo řešení mezi sebou.

Klíčová slova

Dopad, kvantitativní metoda, kybernetická bezpečnost, riziko, riziková analýza.

Abstract

This bachelor thesis deals with the quantitative approach to risk analysis in the framework of cyber security.

The first part is devoted to the theoretical level. There are defined basic terms connected with cyber security and cyberspace. The risk management process according to ISO / IEC 27005 and NIST methodology is described. Furthermore, a comparison of individual risk analysis methods is performed. Finally, examples of quantitative methods are presented and the CIA triad is presented.

The second part of this thesis is dedicated to the QRA method. This method is applied to two devices and probability, impact and risk are calculated. Finally, the evaluation and comparison of both devices is performed.

The benefit of this bachelor thesis is a compiled methodology, which is applicable not only for the determination of the risk itself, but it is also possible to compare individual systems, equipment or solutions among them.

Keywords

Impact, Quantitative Method, Cyber Security, Risk, Risk Analysis.

Bibliografická citace:

ŘEZÁČ, Petr. *Kvantitativní přístup k rizikové analýze v rámci kybernetické bezpečnosti*. Brno, 2019. Bakalářská práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. 55 s. Vedoucí práce Ing. Radek Fujdiak, Ph.D..

Prohlášení autora o původnosti díla

„Prohlašuji, že svou bakalářskou práci na téma Kvantitativní přístup k rizikové analýze v rámci kybernetické bezpečnosti jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

V Brně dne: 20. května 2019

……
podpis autora

Poděkování

Děkuji vedoucímu bakalářské práce Ing. Radku Fujdiakovi, PhD. za účinnou metodickou, pedagogickou a odbornou pomoc a další cenné rady při zpracování mé bakalářské práce.

V Brně dne: 20. května 2019

.……
podpis autora

Obsah

Seznam symbolů a zkratek

CCTA	Central Communication and Telecommunication Agency
CIA	Confidentality, Integrity, Availability
CVSS	Common Vulnerability Scoring System
ENISA	European Network and Information Security Agency
ISO/IEC	International Organization for Standardization
MARION	Metodika analýzy počítačových rizik zaměřená podle úrovní
NIST	Národní institut standardů a technologie
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OGC	Office of Government Commerce
QRA	Analýza kvantitativních rizik

Seznam obrázků

Seznam tabulek

1. Úvod

V současnosti, tedy v 21. století, se informační a komunikační technologie staly nepostradatelnou součástí dnešního moderního životního stylu. Oblast informačních a komunikačních technologií je nejrychleji a nejvíce se rozvíjejícím odvětvím lidské činnosti. Občané jsou denně závislí na informační a komunikační infrastruktuře při řízení společnosti, podnikání a výkonu svých práv a svobod, ale také v soukromém životě [1]. Člověk je zahlcen přemírou informací, elektronikou, vynálezy. Všechny tyto lidské výdobytky přinášejí člověku užitek a usnadňují mu práci a život, ale na druhé straně s sebou nesou i řadu rizik. Rozvojem internetu, IT technologií a chytrých zařízení všeho druhu se člověk ocitá ve stálém větším nebezpečí, kdy tuto oblast zneužívají různé osoby k vlastnímu obohacení. Informace či data a jejich využití v sobě zahrnují značný ekonomický i politický potenciál. Informace a jejich obsah mohou rozhodovat nejen o bytí či nebytí jednotlivce či firmy, ale ve své podstatě jsou schopny ovlivnit celosvětový vývoj [2].

V důsledku stále se měnících podmínek neprobíhá lidská činnost vždy podle plánu a vzniká prostor k negativním jevům. Tyto negativní jevy chápeme jako riziko. Slovo riziko není jen pouhým slovem na papíře, ale jedná se o reálnou hrozbu. Snaha lidstva je minimalizace vznikajících rizik. Abychom ochránili lidské životy, majetek a životní prostředí, je nutná prevence rizik ve všech podobách. V této bakalářské práci se zaměřuji na oblast kybernetické bezpečnosti. V širším slova smyslu pod tímto pojmem můžeme chápat souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru. Bezpečnost se v oblasti kybernetiky stává žhavým tématem současnosti. Využití informačních a komunikačních technologií má však i stinné stránky. Jednou z nich je bezesporu i dynamický nárůst „nového druhu“ trestné činnosti, se kterou je třeba se vypořádat tak, aby nedocházelo k ohrožování a porušování zájmů společnosti [2]. Lidská činnost se stává závislou na moderních technologiích, které se neobejdou bez připojení k internetu, tedy bez vzájemného sdílení dat a informací. Informace je nutné chránit před narušením důvěrnosti, dostupnosti a integrity a to během celého jejich životního cyklu. Abychom ochránili svá data a informace, počítačoví experti pracují na vývoji nových bezpečnostních systémů. V dnešní době vznikají nové postupy a metody, jak kybernetické riziko rozpoznat, určit jeho míru, dopad a rozsah případných škod. Tímto tématem se zabývá analýza rizika.

Tato bakalářská práce má za cíl seznámit čtenáře s oblastí rizikové analýzy v rámci kybernetické bezpečnosti. V první části se čtenáři seznámí s problematikou v teoretické rovině. Jsou zde vysvětleny základní pojmy, jako je kybernetický prostor, kybernetická bezpečnost, riziko nebo krize. Tyto pojmy jsou důležité pro pochopení problematiky. V další části je popsán proces řízení rizika, analýza rizika a její metody se zaměřením na kvantitativní metody analýzy rizika včetně softwarových podpor. Hlavním cílem této bakalářské práce je vytvoření a použití kvantitativní metody analýzy rizika a její následná praktická aplikace na dvě aplikace. Na závěr je provedeno finálních srovnání a je vytvořen softwarový nástroj pro realizaci dané metodiky sloužící pro kvantitativní kybernetickou rizikovou analýzu. Výsledkem je metodika uplatnitelná pro vyčíslení rizika i pro porovnání jednotlivých řešení mezi sebou.

2. Kybernetický prostor a jeho bezpečnost

Kybernetický prostor je chápán jako prostor pro vznik, zpracování a výměnu informací, který je tvořen informačními systémy, službami a sítěmi elektronických komunikací. Je možné ho chápat jako metaforu vyjádření virtuálního (nefyzického) prostředí vytvořeného propojením počítačových systémů v síti. Probíhá zde vzájemné působení mezi subjekty stejně jako v reálném světě, ovšem bez nutnosti fyzické aktivity [1]. Sdílení informací probíhá v reálném čase či s určitým zpožděním. Kybernetický prostor lze také definovat jako prostředí, v němž se informace vytvářejí, zpracovávají, ukládají nebo šíří pomocí elektromagnetického vlnění [1]. Obecně si ho lze představit jako virtuální svět vytvořený moderními technologickými prostředky.

V současnosti bývá termín kybernetického prostoru vykládán různými způsoby. Je obtížné najít stoprocentně platnou definici, která by zahrnovala vše a kterou by bylo možné jednotně a bez výjimek používat. I když se některé názory liší, většina definic se shoduje v tom, že kybernetický prostor je nefyzickým místem, kde se nacházíme během komunikace zprostředkovanou moderními technologiemi (např. počítačem) [1]. Využívání kybernetického prostoru a souvisejících technologií v dnešní době ovlivňuje celou společnost. Význam sociálních sítí pro sdílení informací a pro virtuální kontakt s přáteli představuje zcela nový rozměr.

Mezi hlavní nejasnosti kybernetického prostoru lze zařadit rozměr, hranice, pravomoc a odpovědnost. Stejně jako virtuální realita prezentuje kybernetický prostor virtuální světy, ve kterých se mohou uživatelé či návštěvníci pohybovat a které mohou prozkoumávat. Nemá ale přesně určený rozměr. Jedná se o síť navzájem propojených počítačů bez začátku a konce [1]. Co se hranic týče, kybernetický prostor nemá ve skutečnosti žádné smysluplné geografické hranice. Kybernetickou bezpečnost pak vlády vyspělých států vnímají jako národní politickou záležitost, protože nezákonné použití kyberprostoru může bránit rozvoji hospodářské, ekonomické a národní bezpečnostní činnosti. Vládní představitelé jsou zodpovědní za kybernetickou bezpečnost [1]. Pro kyberprostor je příznačné, že se do něj propojila značná část společnosti. K masovému zapojení společnosti začalo docházet teprve před cca 15 až 20 lety.

2.1 Pojetí kybernetického prostoru

Pojetí kybernetického prostoru se postupně vyvíjelo v čase. Během vývoje převládaly různé názory ohledně pojetí kyberprostoru. Pro názornost jsem vybral několik zástupců. Je to rozčleněno a pojmenováno podle autorů názorových myšlenek. Pojetí kybernetického prostoru můžeme tedy následně členit [1] [3]:

- Gibsonovo pojetí
  Pojem kybernetický prostor pochází od amerického spisovatele sci-fi, Williama Gibsona, který ho použil ve svém románu Neuromancer z roku 1984. Gibsonova metaforická vize se stala inspirací pro tvůrce počítačových systémů a jejich uživatelských rozhraní.
- Barlowovo pojetí
  Kybernetický prostor lze označit jako jakýkoliv deteritorializovaný, symbolický prostor mediované komunikace, jehož komplexnost záleží pouze na úrovni složitosti technologie, co ji zprostředkovává.

- Hakkenovo pojetí
  Charakterizuje kybernetický prostor jako sociální arénu, do které vstupují všichni sociální aktéři používající pokročilé informační technologie ke vzájemné sociální interakci. Dále ho přirovnává k životnímu stylu nebo ke kultuře vytvořené pokročilými informačními technologiemi.
- Pojetí Computer Science and Communications Dictionary
  Definuje kybernetický prostor jako nehmotný svět informací, který vzniká vzájemným propojením informačních a komunikačních systémů. Toto prostředí umožňuje vytvářet, uchovávat, využívat a vzájemně si vyměňovat informace. Také zahrnuje počítače a databáze propojené komunikačními systémy jako například celosvětovou síť Internet.
- Pojetí Lea Troye
  Připisuje kybernetickému prostoru nové možnosti komunikace, jako jsou například e-maily, webové stránky, počítačové sítě, telefony, faxy a videokonference.
- Pojetí Sofie Tzimopoulouové
  Popisuje kybernetický prostor jako imaginární místo, na které se nevztahují omezení fyzického světa. Také umožňuje vznik nových identit. Uživatel opouští své fyzické tělo a pobývá v tomto prostředí bez něj.

2.2 Kybernetická bezpečnost

Pojem kybernetická bezpečnost je v různých zdrojích definován různě, v širším slova smyslu však pod tímto pojem můžeme chápat souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru [4]. Kybernetická bezpečnost pomáhá identifikovat, hodnotit a řešit hrozby v kyberprostoru, snižovat kybernetická rizika a eliminovat dopady kybernetických útoků, informační kriminality, kyberterorismu a kybernetické špionáže ve smyslu posilování důvěrnosti, integrity a dostupnosti dat, systémů a dalších prvků informační a komunikační infrastruktury. Hlavním smyslem kybernetické bezpečnosti je tedy ochrana prostředí k realizaci informačních práv člověka [5].

Kybernetická bezpečnost chrání systémy před kybernetickými hrozbami. Tyto hrozby jsou realizovány v kybernetickém prostoru. Pod pojmem hrozba v kybernetickém prostoru si možno představit potenciální příčinu nežádoucí události, která může mít za následek poškození systému a jeho aktiv, např. zničení, nežádoucí zpřístupnění (kompromitace), modifikaci dat nebo nedostupnost služeb [4]. Mohou být úmyslné (malicious) a neúmyslné (nonmalicious). Úmyslné hrozby jsou realizovány s cílem úmyslně ohrozit bezpečnost. Jsou známé jako útoky se záměrem jednotlivé systémy přetížit a zamezit tak jejich fungování. Neúmyslné hrozby pramení z poškození zařízení nebo vlivem chyby v programu. Jejím cílem je zejména ochrana informačních a infrastrukturních aktiv. V současnosti je obtížné vymyslet dlouhodobě použitelné opatření kybernetické bezpečnosti, neboť existuje více zařízení než lidí, útočníků stále přibývá a vymýšlejí rafinovanější útoky. Lidé, postupy a technologie musí spolupracovat k dosažení efektivní ochrany před hrozbami.

2.2.1 Kybernetická versus informační bezpečnost

Informační bezpečnost zajišťuje důvěrnost, integritu a dostupnost informací. Pro zajištění bezpečnosti musejí být informace ve všech podobách ochráněny před hrozbami a původci hrozeb v jakékoli podobě [6]. Předmětem ochrany z pohledu informační bezpečnosti jsou informace bez ohledu na to, zda jsou uloženy v informačním systému, vytištěny na papíře nebo existují pouze v něčí mysli. V oblasti bezpečnosti informačních systémů se setkáváme s určitými obtížemi, které vznikají jako důsledek dynamických změn rizikových faktorů a prudkého vývoje informačních technologií. Nevezmeme-li v úvahu všechny faktory rizika, může to vést k neefektivním a zbytečně drahým opatřením. Zvládání rizik musí být považováno za jeden z rozhodujících kroků řešení bezpečnosti.

Kybernetická bezpečnost se zabývá ochranou před hrozbami, které využívají kybernetický prostor. Takové hrozby mohou útočit na informační aktiva, proto je informační bezpečnost důležitou součástí kybernetické bezpečnosti. Kybernetická bezpečnost se ale zabývá jen takovými informačními aktivy, ke kterým se dá získat přístup pomocí kybernetického prostoru. Kybernetická bezpečnost se ale neomezuje jen na ochranu informačních aktiv. Její starostí je i ochrana infrastruktury a v širším kontextu [6]. Mnoho zdrojů k tématu kybernetické bezpečnosti pak propojuje kybernetickou a informační bezpečnost. Pro správné pochopení principů kybernetické bezpečnosti je ale nutné tyto pojmy nezaměňovat: kybernetická bezpečnost má mnohem širší zásah, neslouží jen k ochraně informačních aktiv a zajištění jejich důvěrnosti, integrity a dostupnosti informací. Podobně informační bezpečnost není rozsahem omezena na hrozby, které vznikají v kybernetickém prostoru.

2.2.2 Standardy kybernetické a informační bezpečnosti

Norma ISO/IEC 27000 je zavedená řada standardů pro zabezpečení informací. Rozsah uplatnění těchto norem může být pro organizaci jako celek, jednotlivé obchodní procesy nebo dokonce IT aplikace či IT infrastruktury [7]. Norma ISO/IEC 27005 popisuje proces řízení rizika informační bezpečnosti. Tato mezinárodní norma podporuje koncept ISO/IEC 27001 a je navržena tak, aby napomáhala efektivní implementaci informační bezpečnosti založené na řízení rizik. Norma obsahuje následující kapitoly – základní informace, stavba procesu řízení rizik, vytvoření kontextu, vyhodnocení rizika, ošetření rizika, akceptace rizika, monitorování rizika, identifikace a ohodnocení aktiv a dopadu, hrozby a zranitelnost [8].

Národní institut standardů a technologie (NIST) vydal doporučení a speciální publikaci pro řízení rizik systémů informačních technologií. V publikaci je v devíti krocích popsána metoda vyhodnocení rizika [9]. Činnosti NIST jsou organizovány do laboratorních programů, které zahrnují vědu a technologii nanometrů, inženýrství, informační technologie, výzkum neutronů, měření materiálů a fyzikální měření.

Ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany je Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB). Vznikl 1. srpna 2017 na základě zákona č. 205/2017 Sb., kterým se změnil zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (Zákon o kybernetické bezpečnosti) [10].

2.3 Kybernetický bezpečnostní incident

Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) v §8 odstavci 2 je kybernetický bezpečnostní incident definován takto: „Jedná se o narušení bezpečnosti informací a služeb v informačních systémech nebo integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události [11].“ Tato definice uvádí, že došlo k porušení bezpečnostních politik a jasně se distancuje od narušení bezpečnosti v důsledku přírodních pohrom nebo výpadku proudu. Výkladový slovník kybernetické bezpečnosti definuje pojem kybernetický bezpečnostní incident takto: „Porušení nebo bezprostřední hrozba porušení bezpečnostních politik, bezpečnostních zásad nebo standardních bezpečnostních pravidel provozu informační a komunikační technologie [4].“

2.3.1 Typy kybernetický bezpečnostních incidentů

Kybernetických bezpečnostních incidentů zaznamenáváme velké množství a mají mnoho příčin, pro větší přehlednost je rozdělujeme podle příčiny a podle dopadu [12]. Rozdělení podle příčiny: incident způsobený kybernetickým útokem nebo jinou událostí vedoucí k průniku do systému nebo k omezení dostupnosti služeb, incident způsobený škodlivým kódem, incident způsobený překonáním technických opatření, incident způsobený porušením organizačních opatření, incident spojený s projevem trvale působících hrozeb [12]. Toto jsou kybernetické bezpečnostní incidenty, které mají konkrétní příčinu v porušení kybernetické bezpečnosti.

Kybernetické bezpečnostní incidenty rozdělujeme také podle jejich dopadu: incident způsobující narušení důvěrnosti aktiv, incident způsobující narušení integrity aktiv, incident způsobující narušení dostupnosti aktiv a také na incident způsobující kombinaci dopadů uvedených v předcházejících bodech [12]. Tyto kybernetické bezpečnostní incidenty nám působí především na aktiva a působí na CIA triádu (důvěrnost, integrita, dostupnost).

2.3.2 Kategorie kybernetických bezpečnostních incidentů

Kybernetické bezpečnostní incidenty, které chápeme jako porušení bezpečnosti informací a služeb v informačních systémech, rozdělujeme je podle závažnosti. Jsou rozděleny celkem do tří kategorií. Níže jsou vypsány jednotlivé kategorie včetně jejich popisu závažnosti a jejich řešení [12]:

- Kategorie I – méně závažný incident, při kterém dochází k méně významnému narušení bezpečnosti poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje zásahy obsluhy s tím, že musí být vhodnými prostředky omezeno další šíření kybernetického bezpečnostního incidentu včetně minimalizace vzniklých škod.
- Kategorie II – závažný incident, při kterém je narušena bezpečnost poskytovaných služeb. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být vhodnými prostředky zabráněno dalšímu šíření kybernetického incidentu včetně minimalizace vzniklých škod.
- Kategorie III – velmi závažný incident, při kterém je přímo a významně narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být všemi dostupnými prostředky zabráněno dalšímu šíření kybernetického bezpečnostního incidentu včetně minimalizace vzniklých i potenciálních škod.

2.3.3 Řízení bezpečnostních incidentů

V případě, že dojde k bezpečnostnímu incidentu, je nutné ho řešit jednak reaktivně (náprava škod) a jednak proaktivně (přehodnocení celého systému informační bezpečnosti). Systém řízení bezpečnostních incidentů má za úkol detekci bezpečnostní události. Technické prostředky se správně nastavenými metrikami a uživateli s bezpečnostním povědomím. Na správném vyladění obou detekcí závisí efektivita dalších činností. Systém detekce bezpečnostních událostí musí být řádně zdokumentován a musí obsahovat co nejvíce informací o události. Další úkol je identifikace bezpečnostního incidentu, tzn. vyhodnocení nahlášené události, a jestli svým působením vyvolala bezpečnostní incident a posledním úkolem je provedení reaktivního opatření pro snížení nebo odstranění následků incidentu [13].

2.4 Krize

Odvozeno od slova „Krizis“, které pochází z řeckého slova „krino“ znamenající rozhodný okamžik nebo časový úsek, po něm následuje změna ve vývoji děje nebo systému. Je to velmi složitý stav v životě společnosti, v lidské činnosti či v technologických procesech. Negativní důsledky mohou ohrozit existenci, případně jejich funkci. Známé jsou také pojmy mimořádná událost a krizová situace.

2.4.1 Krizová situace

Krizová situace je situace, která vzniká působením činností člověka, přírodními živly a ohrožuje životy, zdraví, majetek nebo životní prostředí. Je vyžadováno uskutečnění záchranných a likvidačních prací. Při narušení infrastruktury nebo při jiném nebezpečí je vyhlášen stav nebezpečí, nouzový stav nebo stav ohrožení státu. Krizové situace lze rozdělit podle příčiny vzniku na krizové situace zapříčiněné člověkem (antropogenní). Sem patří provozní havárie, havárie spojené s infrastrukturou a vnitrostátní společenské, sociální a ekonomické krize. Dále jsou situace zapříčiněné přírodními vlivy, a to živelné pohromy a hromadné nákazy.

2.4.2 Kybernetická krizová situace

Krize je situace, ve které je významný způsobem narušena rovnováha mezi základními charakteristikami systému na jedné straně a postojem okolního prostředí na straně druhé [4]. Krizová situace je mimořádná událost podle zákona o integrovaném záchranném systému, narušení kritické infrastruktury nebo jiné nebezpečí, při nichž je vyhlášen stav nebezpečí, nouzový stav nebo stav ohrožení státu [4]. Ke kybernetickým krizovým situacím dochází v kybernetickém prostoru. Kybernetická krizová situace je situace, kdy dojde ke kybernetickému bezpečnostnímu incidentu. Vzniká jako důsledek kybernetického útoku. Kybernetický útok je činnost, při které je záměrem útočníka získat, modifikovat nebo zničit data (informace), negativně ovlivnit nebo převzít kontrolu nad prvky infrastruktury systému kybernetického prostoru. Kybernetické útoky se stávají stále častějšími a organizovanějšími. Odstraňování jejich následků a škod je stále nákladnější. Takto způsobené škody mohou dosáhnout úrovně, která může ohrozit prosperitu, bezpečnost a stabilitu státu nebo organizace (případně jedince) [14]. Pro úspěšné zvládnutí kybernetické krizové situace je nezbytné nejdříve definovat úrovně kybernetické bezpečnosti, dále je nutno vytvořit tým pro řešení vzniklé krizové situace, dále vytvořit krizový plán a nakonec školit zaměstnance, jak se chovat v krizové situaci.

3. Proces řízení rizik

V této kapitole je nejdříve vysvětlen pojem riziko a jeho definice. Dále jsou podrobně rozepsány jednotlivé kroky procesu řízení rizik s následným popisem metodiky řízení rizik podle doporučení Národního institutu standardů a technologie (NIST). Tento proces je nezbytností pro správné fungování společnosti. Při správném provedení dokáže ušetřit finanční prostředky.

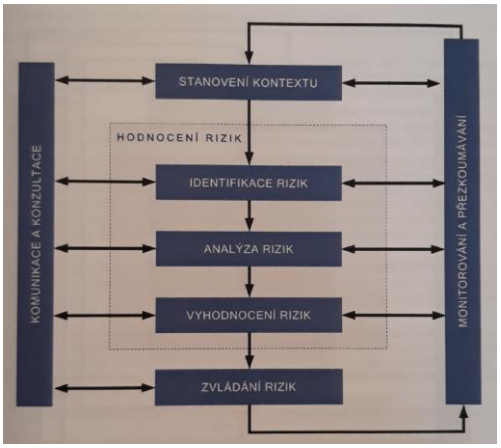
3.1 Riziko

Pojem riziko můžeme definovat jako pravděpodobnost výskytu ztráty při dosahování cílů. Riziko je třeba chápat jako váženou hodnotu, nikoliv absolutní hodnotu. Váha rizika je založena na rozsahu ztráty vzhledem k riziku. Riziko je kombinace pravděpodobnosti a rozsahu ztráty. Některé procesy jsou nekontrolovatelné a výsledky jsou nepředpokládatelné. Definice rizika může být následující: riziko je pravděpodobnost výskytu nežádoucí události při dosahování cílů anebo také definice: pravděpodobnost, že hrozba zneužije zranitelnost a způsobí narušení důvěrnosti, integrity nebo dostupnosti [15].

3.2 Řízení rizik

Řízení rizik je proces v managementu řízení rizik, který napomáhá organizaci vytvářet hodnoty pro její zainteresované strany s optimálním využitím zdrojů organizace, a tím optimalizovat náklady vzhledem k dosahované hodnotě [1]. Hodnocení rizik zahrnuje tři procesy – identifikace rizika, analýza rizika a jeho vyhodnocení. Je to proces, který umožňuje IT manažerům udržet rovnováhu mezi provozními a ekonomickými náklady na ochranná opatření a dosažením zisků při činnosti organizace. Cílem je snižování rizika a zvyšování odolnosti vůči hrozbám vnějšího světa. Správně strukturovaná metodika řízení rizik při efektivním využití napomáhá managementu činit správná rozhodnutí a uskutečnit správná bezpečnostní opatření. Riziko je funkcí pravděpodobnosti daných hrozeb ovlivněných zranitelností a výsledným dopadem nepříznivě ovlivňující společnost [9].

Řízení rizik by mělo být nepřetržitým procesem. Tento proces by měl stanovit kontext, vyhodnotit rizika a ošetřit rizika za použití plánu ošetření rizik pro zavedení doporučení a rozhodnutí. Řízení rizik analyzuje, co se může stát a jaké mohou být případné důsledky, před rozhodnutím, co by se mělo provést a kdy za účelem redukce rizika na přijatelnou úroveň. Proces řízení rizik bezpečnosti informací dle Obr. 1 normy ISO/IEC 27005 sestává ze stanovení kontextu, identifikace, analýzy, vyhodnocení rizik, komunikace rizik a monitorování a přezkoumávání rizik [16].



Obr. 1: Proces řízení rizik **[16].**

3.2.1 Popis systému

Při řízení rizik IT systému v metodice dle doporučení NIST je prvním krokem definice rozsahu. V tomto kroku se identifikují hranice IT systému spolu s prostředky a informacemi, které systém utváří. Charakteristika IT systému stanovuje rozsah řízení rizik, popisuje hranice autorizace a poskytuje nezbytné informace pro definování rizika [9].

3.2.2 Identifikace hrozby

Hrozba je náhodná nebo úmyslně vyvolaná událost s možným negativním dopadem na důvěrnost, integritu a dostupnost aktiv, která může využít zranitelnosti systému. Abychom mohli čelit hrozbám, musíme nejdřív provést tzv. identifikaci hrozeb, tedy zjistit, které to jsou. Většina informačních systémů jsou obvykle vystaveny stejným hrozbám (obecným neboli generickým hrozbám), jejich výčet bývá uveden v nejrůznějších metodikách [17]. Cílem tohoto kroku je identifikace potenciálních hrozeb a sepsání seznamu jednotlivých hrozeb, které jsou aplikovatelné na IT systém [9]. Je důležité přidat do seznamu i specifické hrozby, které ohrožují daný systém.

Dělení hrozeb

Podle úmyslu:

- náhodné hrozby (accidental threat) – jedná se o hrozby, které byly způsobeny zcela náhodně (původce hrozby se označuje jako threat event),
- úmyslné hrozby (deliberate/intentional threat) – jedná se o hrozby, které byly naplánovány (původce hrozby se označuje jako threat agent),
- environmentální hrozby (environmental threat) – zahrnují všechny typy hrozeb od přírodních přes technologické až po sociální.

Podle zdroje:

- vnitřní hrozby (internal/insider threat) – zdroj (příčina) hrozby se nachází uvnitř organizace,
- vnější hrozby (external/outsider threat) – zdroj (příčina) hrozby se nachází mimo organizaci.

Kombinací výše uvedeného způsobu dělení získáváme matici, která zachycuje čtyři základní typy hrozeb. Tato matice je zobrazena v **Tab. 1**.

Tab. 1: Matice hrozeb.

hrozby	náhodné	úmyslné
externí	přírodního původu	hacking
interní	technické selhání lidská chyba	sabotáž

3.2.3 Identifikace zranitelnosti

Analýza rizika IT systému musí obsahovat analýzu zranitelností z prostředí. Zranitelnost je jakákoliv slabina v informačním systému, bezpečnostních postupech, interních nařízení nebo implementací, které mohou být ohroženy. Cílem tohoto kroku je vytvořit seznam zranitelností systému, kterých se dá zneužít. Mezi doporučené metody identifikace zranitelností systému patří využití zranitelných zdrojů, rychlost bezpečnostních testů systému a vytvoření kontrolního seznamu bezpečnostních požadavků [9].

3.2.4 Kontrolní analýza

Cílem tohoto kroku je analyzovat opatření, které byly implementovány, nebo které čekají na implementaci, organizace pro minimalizování nebo eliminaci pravděpodobnosti, že daná hrozba využije zranitelnosti systému. Tento krok zahrnuje využití technických a netechnických metod. Technické metody obsahují ochranu hardwaru, softwaru nebo firmwaru. Netechnické metody jsou bezpečnostní strategie, provozní procesy a bezpečnost zaměstnanců a prostředí. Tento krok se neuskuteční, pokud společnost využívá efektivní bezpečnostní opatření, která dokážou hrozbu eliminovat nebo snížit následky škod na minimum [9].

3.2.5 Stanovení pravděpodobnosti

Pravděpodobnost výskytu hrozeb je dána do souvislosti s hodnotou pravděpodobnosti hrozby a pravděpodobností dopadu. V případě nepřátelských hrozeb je hodnocení pravděpodobnosti založeno na záměru, schopnostech a cíle protivníka. Pro jiné než konvenční hrozby lze pravděpodobnostní výskyt odhadnout pomocí historických dat, empirických údajů a jiných faktorů. Pravděpodobnost je vhodné vyhodnocovat za větší časový rámec. Pro odvození celkové pravděpodobnosti, která značí pravděpodobnost využití určité zranitelnosti, je třeba brát v úvahu následující faktory [9]:

- motivace a schopnosti útočníka,
- typ zranitelnosti,
- existence a efektivita současných nastavení.

3.2.6 Analýza dopadu

Cílem tohoto kroku je analyzovat dopady jednotlivých hrozeb. Ve finančním vyjádření je to objem finančních prostředků, které je nutné vynaložit na nápravu škody způsobené hrozbou nebo útokem. Hodnotou dopadu je rozsah škod, které lze očekávat v důsledku zveřejnění, modifikace, narušení, zničení nebo ztráty informací. Před začátkem analýzy dopadu je nezbytné získat následující informace:

- úloha systému,
- důležitost systému a dat,
- citlivost systému a dat.

Tyto informace je možné získat z existující dokumentace organizace. Tato metoda upřednostňuje úrovně dopadu podle aktiv společnosti, které vyplývají z kvalitativního nebo kvantitativního ohodnocení citlivosti a důležitosti. Pokud tato dokumentace neexistuje, citlivost systému a dat lze odvodit podle úrovně zabezpečení pro zachování dostupnosti, integrity, odpovědnosti a důvěrnosti [9].

3.2.7 Stanovení rizika

Cílem tohoto kroku je zhodnotit úroveň rizika IT systému. Pro zhodnocení rizika je nutné stanovit škálu rizik a matici úrovní rizik. Konečná výše rizika je výsledkem vynásobené pravděpodobnosti hrozeb a dopadu. V závislosti na požadavcích a podrobností posouzení rizika můžeme využívat matici 3 x 3, 4 x 4 nebo 5 x 5. Matice rizika nám vygeneruje velmi nízké až velmi vysoké úrovně rizika. Dosažení úrovně velmi vysokého rizika vyžaduje okamžitou reakci v podobě vypnutí systému nebo začlenění testování [9].

3.2.8 Doporučená opatření

Během tohoto kroku procesu jsou poskytnuty doporučená opatření, které by mohly zmírnit nebo odstranit zjištěná rizika. Cílem doporučených opatření je snížit míru rizika na systém IT a jeho dat na přijatelnou úroveň. Při zavádění opatření nebo alternativních řešení je třeba zvážit následující faktory, které minimalizují nebo odstraňují identifikovaná rizika – účinnost doporučených možností, legislativa a regulace, organizační politika, dopad na provoz, bezpečnost a spolehlivost [9].

3.2.9 Výsledná dokumentace

Výslednou dokumentací je zpráva o hodnocení rizik popisující hrozby, zranitelnost, míru rizika a poskytuje doporučená opatření, která směřují k minimalizaci míry rizika [9]. Zpráva o hodnocení rizik pomáhá vrcholovému vedení, majitelům společností rozhodovat o změnách v politice, procedurální, rozpočtové a systémové operaci a řízení.

4. Metody vyhodnocení rizika

Riziko a jeho faktory mohou být hodnoceny různými způsoby, například kvantitativně, kvalitativně nebo semikvantitativně. Každý způsob vyhodnocení rizik má své výhody a nevýhody.

Kvantitativní metody obvykle využívají soubory metod, zásad nebo pravidla hodnocení rizik na základě čísel. U tohoto přístupu se používají číselné hodnoty pro následky i jejich pravděpodobnosti, které se stanoví pomocí údajů získaných z různých zdrojů (statistické ročenky, účetnictví). Základem je používání matematických a statistických metod. Výsledná kvalita analýzy závisí především na přesných a úplných datech [9]. Význam kvantitativních metod však nemusí být vždy jasný a může vyžadovat kvalitativní interpretaci. Výhody kvantitativních metod (z hlediska přesnosti, opakovatelnosti a reprodukovatelnosti) mohou být v některých případech převáženy náklady (z hlediska času a úsilí odborníků a možného zavedení a používání nástrojů, které jsou nezbytné pro taková hodnocení).

Na rozdíl od kvantitativních metod, kvalitativní metody používají soubory metod, zásad nebo pravidla hodnocení rizik na základě nečíselných kategorií nebo úrovní (velmi nízká, nízká, střední, vysoká, velmi vysoká) [9]. Principem je odhad jednotlivých aktiv, hrozeb a zranitelností expertem. Používá se nečíselných údajů k popisu rozsahu možných následků a pravděpodobností. Můžeme používat různé bodové škály, hrozby mohou být vyjádřeny pravděpodobností, nebo mohou být popsány slovy. Metoda je více subjektivní a záleží na znalostech a zkušenostech hodnotitele. Často se vychází z vypracovaných dotazníků či anket a z hodnocení expertů a specialistů z daného oboru [18]. Rozsah hodnot v kvalitativních metodách je ale ve většině případů poměrně malý, což ztěžuje relativní stanovení priorit nebo vzájemné srovnání.

Semikvantitativní metody vytváří přechod mezi kvantitativní a kvalitativní analýzou. Jsou založeny na expertním odhadu pravděpodobnosti aktivace zdroje nebezpečí a zranitelnosti ohrožených aktiv. Vyznačují se rychlostí, nižšími požadavky na vstupní data, jednoduchostí provedení a menší náročností na potřebné zdroje. Obvykle využívají soubory metod, zásad nebo pravidla hodnocení rizik podle intervalů, stupnic nebo reprezentativních čísel. Výstupy jsou prezentovány v intervalech pravděpodobnosti a zranitelnosti v matici a mapě rizik [9]. Tento typ hodnocení může poskytnout výhody kvantitativních a kvalitativních hodnocení. V následující Tab. 2 jsou přehledně znázorněny výhody a nevýhody jednotlivých analýz rizika.

Tab. 2: Výhody a nevýhody jednotlivých analýz.

Kvantitativní analýza	Kvalitativní analýza	Semikvantitativní analýza
+ využití speciálních softwarů	+ snadná a rychlá identifikace rizik	+ snadná a rychlá identifikace rizik
+ spolehlivé výstupy	− neposkytuje měřitelné charakteristiky nebezpečí a dopadu	− výstupy subjektivního charakteru
− náročná na vstupní finanční zdroje	+ nižší cena	+ pokrývá širší rozsahy pravděpodobnosti a dopadu
− omezené použití v praxi	+ nižší požadavky na vstupní data a vybavení	+ nižší požadavky na vstupní data a vybavení
− časově velice náročná	+ vyznačuje se rychlostí provedení	+ vyznačuje se rychlostí provedení
+ lepší kontrola nákladů procesu	− vyžaduje dokonalou znalost prostředí	− nižší správnost a spolehlivost výstupů
+ přesnější, správnější a spolehlivější výstupy	− nižší přesnost	− nižší přesnost

4.1 Příklady kvantitativních metod

V současné době se riziko kybernetického útoku rapidně zvyšuje a současné metodiky jsou již nedostatečné, proto se neustále vyvíjejí nové a sofistikovanější metody k analýze rizik. Níže jsou představeny některé kvantitativní metody kybernetické analýzy rizika.

- **Monte Carlo** analýza je podobná scénáři „co kdyby“ v tom, že vytváří řadu možných scénářů. Jedná se však o krok navíc tím, že efektivně zachycuje každou možnou hodnotu, kterou může každá proměnná přijmout, a váží každý možný scénář pravděpodobností jejího výskytu. QRA toho dosáhne tím, že modeluje každou proměnnou v modelu pravděpodobnosti. Struktura modelu QRA je obvykle velmi podobná deterministickému modelu. Propojující proměnné dohromady, kromě toho, že každá proměnná je reprezentována funkcí distribuce pravděpodobnosti jedné hodnoty. Cílem QRA je vypočítat kombinovaný dopad nejistoty v parametrech modelu, aby bylo možné určit rozložení nejistot možných výsledků modelu [19].
- **Heuristická metoda** je přístup k nalezení řešení problému, který pochází ze starověkého řeckého slova „hurisko“, což znamená „najít“, „hledat“ nebo „objevit“. Heuristické metody urychlují proces dosažení uspokojivého řešení. Využívají techniky založené na zkušenostech nebo odborných znalostech k odhadu nepředvídané události. Patří zde např. Procento celkových hodnot nebo procento vážených aritmetických průměrů [20].
- **Očekávaná hodnota** je základním pojmem v kategorii pravděpodobnosti v matematice. Očekávaná hodnota proměnné je definována jako průměrná hodnota, která je intuitivní v dlouhodobé hodnotě opakovaným prováděním experimentu, který reprezentuje. Můžeme říci, že očekávání diskrétního druhu náhodných proměnných je vážená průměrná pravděpodobnost hodnot, které jsou možné. Pro získání hodnoty nepředvídané události se vynásobí pravděpodobnost rizika maximálním časem (náklady) na odhalení rizika. Patří zde např. Metoda momentů nebo Očekávaná hodnota jednotlivých rizik [21].

- **Metoda „Probability Distribution“** udává pravděpodobnost události nebo výsledku. Součet všech pravděpodobností pro všechny možné hodnoty se musí rovnat 1. Navíc pravděpodobnost pro určitou hodnotu nebo rozsah hodnot musí být mezi 0 a 1. Distribuce pravděpodobnosti popisuje rozptyl hodnot náhodné proměnné. V důsledku toho druh proměnné určuje typ rozdělení pravděpodobnosti [22].
- **Metoda QuERIES** se skládá ze sedmi kroků a byla úspěšně aplikována na různé kybernetické situace. Metoda se člení na čtyři základní skupiny [23]:
    1. Modelace problému – obsahuje ekonomické hodnoty duševního vlastnictví (ochranu softwaru), náklady na udržování duševního vlastnictví, mapu specifických ochran duševního vlastnictví.
    2. Modelace útoků – použití ochranné mapy a znalostí metod reverzního inženýrství k vytvoření grafu útoku.
    3. Kvantifikace modelů – vytvoření speciálního týmu na ochranu duševního vlastnictví proti útokům a dalšího týmu na odhad parametrů.
    4. Využití výsledků – výsledné odhady mohou být použity pro rozhodování, zda jsou navrhované ochrany vhodné pro konkrétní zranitelnosti z hlediska různých možných analýz nákladů a přínosů.

4.2 Nástroje na podporu analýzy rizik

ENISA (European Network and Information Security Agency) vytvořila v roce 2006 základ pro inventář metod a nástrojů na management a vyhodnocení rizik, který je publikovaný přímo na webové stránce ENISA [24]. Aby bylo možné vzájemné porovnání vlastností metod a nástrojů, byly vytvořeny pro jednotlivé metody a nástroje samostatné šablony obsahující posuzované atributy. Níže jsou představeny některé metody.

- **CRAMM** je metoda analýzy rizik vyvinutá britskou vládní organizací CCTA (Central Communication and Telecommunication Agency), nyní přejmenovanou na Office of Government Commerce (OGC). Nástroj se stejným názvem podporuje metodu: CRAMM. V současné době je CRAMM výhodnou metodou analýzy rizik ve vládě Spojeného království. CRAMM je vhodný zejména pro velké organizace, jako jsou státní orgány a průmysl [25].
- Metoda **MEHARI Expert** poskytuje kompletní model řízení rizik vyhovující požadavkům ISO 27005. Zahrnuje klasifikaci majetku, pravděpodobnost hrozeb a opatření zranitelnosti prostřednictvím auditu. Dále analyzuje seznam obecných rizikových situací a poskytuje úroveň závažnosti pro každý scénář. Svou analýzu zakládá na vestavěné pomoci a parametrech a umožňuje optimální výběr nápravných opatření. Poskytuje dodatečné hodnocení souladu organizací podle pravidel ISO 27002: 2013 [26].
- Metoda **MARION** (Metodika analýzy počítačových rizik zaměřená podle úrovní) vychází z metodiky auditu, která umožňuje odhadnout úroveň bezpečnostních rizik společnosti v podniku prostřednictvím vyvážených dotazníků, které poskytují ukazatele ve formě poznámek k různým tématům týkajícím se bezpečnosti. Úroveň zabezpečení je odhadována podle 27 ukazatelů rozdělených do 6 velkých subjektů, přičemž každá z nich přiděluje stupeň mezi 0 a 4. Na závěr této analýzy se provádí podrobnější analýza rizika s cílem identifikovat rizika (hrozby a zranitelnosti), kterým čelí společnost [27].

- Metoda **CVSS** (Common Vulnerability Scoring System) je volný a otevřený průmyslový standard pro posuzování závažnosti chyb zabezpečení počítačových systémů. CVSS se pokouší přiřadit zranitelnost skóre závažnosti, což umožňuje respondentům upřednostňovat reakce a zdroje podle hrozby. Skóre se vypočítá na základě vzorce, který závisí na několika metrikách, které přibližují snadnost využití a dopadu zneužití. Skóre se pohybuje od 0 do 10, přičemž hodnota 10 je nejzávažnější [28].

4.3 Riziková analýza vs kybernetická riziková analýza

Přístup rizikové analýzy je založen na zjišťování rizik v podnicích a jejich následná odstranění nebo redukce. Podniky musí čelit riziku každý den, je to součástí obchodu hlavně v digitálním světě. Zvládání rizik je klíčový proces pro úspěšný chod firmy. Pokud se firma odmítá zabývat tímto procesem, vystavuje je hrozbám. Proces analýzy rizika při podnikání pomáhá redukovat riziko, potažmo náklady vynaložené na odstranění vzniklého rizika. Společnostem hrozí nejen kybernetické riziko, ale také hrozby přírodního původu nebo náhodné hrozby.

Kybernetická riziková analýza vytváří analýzu hrozeb způsobených v kyberprostoru. To znamená ve virtuálním prostředí vytvořené propojením počítačových systémů v síti. Kybernetická hrozba má vektor útoku, pomocí kterého útočník proniká do systému. Útočník chce získat, modifikovat nebo zničit data (informace), negativně ovlivnit nebo převzít kontrolu nad prvky infrastruktury systému kybernetického prostoru. Kybernetické útoky se stávají stale častějšími a organizovanějšími. Odstraňování jejich následků a škod je stále nákladnější. Analýza má za úkol identifikovat hrozby, zjistit vektory útoku, stanovit dopad a vyčíslit riziko.

4.4 Triáda CIA

Důvěrnost (confidentiality), integrita (integrity) a dostupnost (availability) známe také jako triádu CIA. Prvky této triády jsou považovány za tři nejdůležitější složky bezpečnosti. Důvěrnost je zhruba ekvivalentem slova „soukromí“. Opatření, která jsou zaváděny k zajištění důvěrnosti, se snaží zabránit tomu, aby se citlivé informace nedostaly do nepovolaných rukou a zároveň zajistit, aby dotyčná data mohly prohlížet jen pověřené osoby. Integrita zahrnuje zachování konzistence, přesnosti a důvěryhodnosti dat v celém jejich životním cyklu. V případě integrity je potřeba si uvědomit, že pokud dojde k nežádoucí změně dat, a to ať už úmyslně, náhodou nebo technickým selháním, nemusí být tato nežádoucí změna vůbec odhalena. Dostupnost znamená zajištění, že informace je pro oprávněné uživatele přístupná v okamžiku její potřeby [29].

5. QRA metoda v praxi

Pro praktické znázornění metody jsem vybral dvě zařízení, pro které vypracuji kvantifikační rizikovou analýzu kybernetické bezpečnosti. Jedná se o infuzní pumpu a průmyslového robota, který je součástí industriálního systému.

Infuzní pumpa, Obr. 2, je zařízení, které se používá ve zdravotnictví k přesnému dávkování farmak a krevní infuze a udržování dávkovací rychlosti intravenózní infuze. Disponuje celou řadou pokročilých funkcí a je příkladem technologického pokroku v moderní medicíně a lékařství. V současné době se přístroje užívají nejen na všech odděleních nemocnice, na operačních sálech, ale také ve vozech záchranné služby, poslední modely jsou dokonce certifikovány k využití ve vrtulníku. Toto zařízení je těžko napadnutelné, neboť k němu má přístup pouze omezený počet osob a není připojeno k veřejné počítačové síti. Do budoucna se počítá s tím, že bude možné na dálku navrhnout změnu dávkování infuze, navrhnutou změnu pomocí dálkového ovládání musí ale vždy potvrdit přímo na místě kvalifikovaný zdravotník.

Obr. 2: Infuzní pumpa HK-400 [30].

Průmyslový robot, Obr. 3, je automatický stroj, který obsahuje manipulátor se dvěma a více pohybovými osami a programovatelný řídicí systém na uskutečňování pohybových a řídících funkcí ve výrobním procesu. Tyto stroje nahrazují analogické funkce člověka při přemísťování předmětů a technologického příslušenství. Existuje několik důvodů, proč lidé nasazují průmyslové roboty jako součást výrobního procesu. V první řadě to jsou technické důvody (zlepšení kvality výrobků, snížení zmetkovitosti a pružnost výroby), další jsou ekonomické důvody (zvýšení výrobní kapacity, zvýšení koeficientu směnnosti, úspora pracovního místa a uvolnění kvalifikovaných pracovníků) a na závěr sociální důvody (vyřazení člověka z fyzicky namáhavé a monotónní práce, vyřazení člověka ze zdraví škodlivého prostředí). Je možné je využívat při svařování, lakování, lisování a kování, ve sklářském průmyslu, při paletizaci výrobků, manipulacích a při montáži.

Obr. 3: Průmyslový robot v praxi [31].

5.1 Praktický výpočet

Praktický výpočet pro posouzení rizik se skládá z identifikace analýzy a hodnocení rizik. Posouzení rizik riziko kvantifikuje a umožňuje vedoucím pracovníkům, aby určili prioritu rizik podle stanovených kritérií nebo vnímané důležitosti. Posouzení rizik je podrobněji popsáno v následujících kapitolách.

5.1.1 Identifikace aktiv při praktickém výpočtu

Součástí identifikace rizik je proces identifikace aktiv. Aktivum je cokoliv, co má pro organizaci hodnotu a co tedy vyžaduje ochranu. Identifikace aktiv by měla být provedena na vhodné vstupní podrobnosti, který poskytuje pro posouzení rizik dostatek informací. U každého aktiva by měl být identifikován vlastník aktiva k zajištění záruky a odpovědnosti za aktivum. Vlastník aktiva k němu možná nemá vlastnická práva, ale má přiměřenou odpovědnost za jeho produkci, vývoj, údržbu, používání a bezpečnost. Rozlišujeme dva druhy aktiv – primární (obchodní procesy a činnosti, informace) a podpůrná (hardware, software, sítě, pracovníci, lokalita, organizace).

V mém případě u zařízení infuzní pumpa jsou nadefinovány aktiva: samotné zařízení, hardware, operační systém, specifický software, proškolený personál, pracovníci údržby. Zařízení průmyslový robot má nadefinována aktiva: výrobní proces, technické informace, samotné zařízení, operační systém, specifickou podnikovou aplikaci, komunikační rozhraní, operační paměť, obsluhující personál, pracovníci údržby, vývojáři.

Dalším krokem po identifikaci aktiv je ohodnocení aktiv. Kvůli různorodosti aktiv vyskytujících se ve většině organizací je pravděpodobné, že některá aktiva, která mají známou peněžní hodnotu, budou ohodnocena v místní měnové jednotce, zatímco ostatní aktiva, která mají kvalitativnější hodnotu, mohou být seřazena podle hodnoty např. od „velmi nízké“ po „velmi vysokou“.

5.1.2 Identifikace hrozeb při praktickém výpočtu

Při analýze rizika je důležité správně stanovit hrozby a provést jejich kvantifikaci. Ve své bakalářské práci jsem se pro vybraná zařízení inspiroval výběrem jednotlivých typů hrozeb v normě ISO/IEC 27005. V Tab. 3 jsou uvedeny jednotlivé typy hrozeb u vybraných zařízení. Každé zařízení má několik typů hrozeb, ke kterým jsou přiřazeny jednotlivé faktory hrozeb. V tabulce jsou uvedeny pouze hrozby, které mohou pocházet z kyberprostoru.

Pro svou práci jsem si vybral celkem devět hrozeb, které jsou dále blíže popsány. Hrozba vzdálená špionáž spočívá v získávání strategicky citlivých či strategicky důležitých informací od jednotlivců nebo organizací za použití IT prostředků [4]. Další hrozbou jsou data pocházející z nedůvěryhodných zdrojů. Tato hrozba je velmi zákeřná, neboť v případě použití nedůvěryhodných dat ohrozíme stávající systém. Selhání zařízení může nastat v případě, že obsluha nedodrží stanovený postup nebo špatnou manipulací se zařízením. Zneužití oprávnění je záměrná nebo z nedbalosti plynoucí činnost, která ovlivňuje kybernetickou bezpečnost systému zpracování dat [4]. To znamená, že útočník využije příležitosti k nabourání se do systému a způsobení škody. Další hrozbou je sociální inženýrství spočívající ve způsobu manipulace lidí za účelem provedení určité akce nebo získání určité informace [4]. Pretexting je jeden z druhů sociálního inženýrství, který vytváří a využívá smyšleného scénáře s cílem přesvědčit oběť k učinění potřebné akce či k získání potřebné informace [4]. Chybné fungování zařízení

představuje poruchu uvnitř systému způsobené obsluhou nebo útočníkem. Hacking je činnost spočívající v hledání a využívání bezpečnostních děr v počítačových systémech [4]. Škodlivý virus známe pod pojmem počítačový virus. Je to počítačový program, který se šíří prostřednictvím internetu (elektronická pošta, stahování programů) a replikuje se připojováním své kopie k jiným programům. Může být použit za účelem získání různých typů dat, zcizením identity nebo znefunkčněním počítače [4]. Neoprávněný přístup vzniká překonáním bezpečnostních opatření a umožňuje získat nekontrolovatelnou moc nad systémem.

Tab. 3: Jednotlivé typy hrozeb u infuzní pumpy a průmyslového robota.

Typ	Hrozby
Ohrožení informací	Vzdálená špionáž
	Data pocházející z nedůvěryhodných zdrojů
	Selhání zařízení
	Chybné fungování zařízení
Ohrožení z kyberprostoru	Zneužití oprávnění
	Sociální inženýrství
	Hacking
	Škodlivý virus
	Neoprávněný přístup do systému

5.1.3 Určení pravděpodobnostního výskytu

Pro určení pravděpodobnostního výskytu jednotlivých hrozeb je nutné vycházet ze statistických dat, ročenek, z účetnictví a také z předcházejících analýz. Pro výpočet pravděpodobnosti jsem využil heuristickou metodu, která je založena na zkušenostech a odborných znalostech. Jedná se o simulaci rizika s využitím vážených aritmetických průměrů, která patří k analytickým metodám vytvářených na základě matematicko-statistické a pravděpodobnostní analýzy. Simulaci rizik lze využít v zejména ve fázi analýzy rizik, kdy se určí faktory (příčiny) rizik a provede se expertní odhad jejich pravděpodobností. Při této metodě se pravděpodobnosti oceňují číselně. Tyto odhady pravděpodobností slouží k určení celkové pravděpodobnosti výskytu rizika.

Pro vlastní výpočet pravděpodobnosti jednotlivých hrozeb jsem si určil faktory rizika neboli příčiny rizika a ke každému faktoru je i přiřazena jeho váha. Jelikož nemám přístup k historickým datům ani ke statistickým ročenkám, proto jsou moje použitá čísla pouze orientační na základě mých znalostí. Vzorová tabulka pro výpočet výskytu hrozeb u optimistického a pesimistického scénáře s názvem „Vzorová tabulka pro výpočet výskytu hrozeb“ je uvedena v příloze 1. Z jednotlivých pravděpodobnostních faktorů se vypočte výsledná pravděpodobnost hrozby pomocí váženého aritmetického průměru podle vzorce **(5.1)**:

$$P_h = \frac{\sum_{i=1}^{m} P_{fi} * v_{fi}}{\sum_{i=1}^{m} v_{fi}} \tag{5.1}$$

kde P_h je pravděpodobnost hrozby, P_{fi} je pravděpodobnost výskytu i-tého faktoru a v_{fi} je váha i-tého faktoru.

Pro přesnější výsledné číslo jsem se rozhodl stanovit dva možné scénáře pravděpodobnosti výskytů hrozby, a to optimistický a pesimistický scénář. Optimistický scénář P_{opt} znamená minimální možnou pravděpodobnost výskytu hrozby, a naopak pesimistický scénář P_{pes} znamená největší možnou pravděpodobnost, že hrozba nastane. U jednotlivých hrozeb vezmeme vypočtené vážené aritmetické průměry u obou scénářů (optimistické i pesimistické výskytu) a vypočteme jejich aritmetické průměry pomocí vzorce (5.2). Tím dostaneme výslednou hodnotu pravděpodobnosti jednotlivých hrozeb.

$$\bar{x} = \frac{1}{n}\sum_{i=1}^{n} x_i \tag{5.2}$$

5.1.4 Určení zranitelnosti a dopadu

Dalším krokem analýzy rizika je určení zranitelnosti a dopadu rizika. Zranitelnost je slabina v systému, kterou může útočník využít ve svůj prospěch. Dopad je důsledkem nechtěného incidentu, který ovlivňuje aktiva. Takové důsledky by mohly být zničení některých aktiv, poškození systému IT a ztráty důvěrnosti, integrity, dostupnosti, odpovědnosti nebo spolehlivosti. Dopad může být měřen jak kvantitativně (např. odhadováním finančních nákladů), tak kvalitativně. Dopad se považuje za takový, který má buď okamžitý (provozní) účinek, nebo budoucí (obchodní) účinek, který zahrnuje finanční a tržní následky.

Pro výpočet hodnoty zranitelnosti a dopadu rizika jsem si vybral metodiku CVSS Calculator 3.0 [32]. Tato metodika poskytuje způsob, jak zachytit hlavní charakteristiky zranitelnosti a vytvořit numerické skóre odrážející jeho závažnost. Je to kvantitativní model zajišťující opakovatelné přesné měření a umožňuje uživatelům vidět základní charakteristiky zranitelnosti a dopadu, které byly použity pro generování skóre. Systém CVSS je volně přístupný pro posuzování závažnosti hrozeb v kybernetickém prostoru. Přiřazuje zranitelnosti a dopadu skóre závažnosti, což umožňuje uživatelům upřednostňovat reakce a zdroje podle hrozby. Skóre se počítá na základě vzorců (5.3) a (5.4):

$$ISC_{Base} = 1 - [(1 - Impact_{Conf}) * (1 - Impact_{Integ}) * (1 - Impact_{Avail})] \tag{5.3}$$

$$Exp = 8{,}22 * AttackVector * AttackComplexity * PrivilegeRequired * UserInteraction \tag{5.4}$$

kde ISC_{Base} je základní skóre dopadu, $Impact_{Conf}$ je dopad důvěrnosti, $Impact_{Integ}$ je dopad integrity a $Impact_{Avail}$ je dopad dostupnosti.
kde *Exp* je zneužitelnost, *AttackVector* je přístupový vektor, *AttackComplexity* je složitost útoku, *PrivilegeRequired* je požadovaná oprávnění a *UserInteraction* je interakce uživatele. Vzorce závisí na několika metrikách, které přibližují snadnost využití a dopadu zneužití. Skóre se pohybuje od 0 do 10, přičemž 10 je nejzávažnější [28].

Dále jsou uvedeny tabulky pro výpočet zranitelnosti a dopadu. V Tab. 4 s názvem „Přístupový vektor“ vektor ukazuje, jak lze využít útoku. Tab. 5 s názvem „Složitost útoku“ nám popisuje, jak snadné, nebo obtížné je zneužití. Tab. 6 s názvem „Požadovaná oprávnění“ nám znázorňuje úroveň oprávnění, které musí útočník mít, než úspěšně provede útok. Tato metrika je největší, pokud nejsou požadována žádná oprávnění. Tab. 7 s názvem „Interakce uživatele“ zachycuje požadavek, aby se uživatel účastnil úspěšného útoku. V Tab. 8 s názvem „Rozsah“ je znázorněna schopnost zranitelnosti v jedné softwarové komponentě ovlivnit zdroje nad rámec jejich prostředků a oprávnění. Tento důsledek je reprezentován metrickým rozsahem autorizace nebo jednoduše rozsahem. Pro měření dopadu vyplníme **Tab. 9**, která popisuje dopad

na důvěrnost údajů zpracovávaných systémem. Dále vyplníme Tab. **10** popisující dopad na integritu napadeného systému a následující Tab. **11** obsahuje dopad na dostupnost systému. Těchto osm metrik se používá pro výpočet dílčího skóre zranitelnosti a dopadu. Tyto dílčí skóre se následně použijí pro výpočet celkového základního skóre, které využijeme pro výpočet míry rizika [33].

Tab. 4: Přístupový vektor.

Hodnota	Popis	Skóre
Fyzický (Physical - P)	Vyžaduje fyzický přístup útočníka.	0,200
Místní (Local – L)	Útočník musí mít buď fyzický přístup ke zranitelnému systému, nebo lokální účet.	0,550
Sousední síť (Adjacent Network – A)	Útočník musí mít přístup k vysílané nebo kolizní doméně zranitelného systému.	0,620
Síť (Network – N)	Tyto typy útoku jsou často popisovány jako vzdáleně využitelné.	0,850

Tab. 5: Složitost útoku.

Hodnota	Popis	Skóre
Vysoký (High – H)	Existují speciální podmínky a požadavky na metody sociálního inženýrství.	0,440
Nízký (Low – L)	Neexistují žádné zvláštní podmínky pro zneužití.	0,770

Tab. 6: Požadovaná oprávnění.

Hodnota	Popis	Skóre
Žádný (None – N)	Útočník nevyžaduje žádný přístup k provedení útoku.	0,850
Nízký (Low – L)	Útočník má oprávnění, která poskytují základní uživatelské funkce.	0,620
Vysoký (High – H)	Útočník má oprávnění, která poskytují administrativní kontrolu.	0,270

Tab. 7: Interakce uživatele.

Hodnota	Popis	Skóre
Žádný (None – N)	Citlivý systém může být využíván bez interakce jakéhokoliv uživatele.	0,850
Požadovaný (Required – R)	Úspěšné zneužití vyžaduje, aby uživatel provedl nějakou akci dříve.	0,620

Tab. 8: Rozsah.

Hodnota	Popis	Skóre
Beze změny (Unchanged – U)	Útok může ovlivnit pouze prostředky spravované stejným oprávněním.	0,642
Změna (Changed – C)	Útok může ovlivnit i prostředky s vyšším oprávněním.	0,752

Tab. 9: Dopad důvěrnosti.

Hodnota	Popis	Skóre
Žádný (None – N)	Neexistuje žádný vliv na důvěrnost systému.	0,000
Nízký (Low – L)	Existuje značné zveřejnění informací, ale rozsah ztráty je omezen tak, že ne všechny údaje jsou k dispozici.	0,220
Vysoký (High – H)	K dispozici je úplné zpřístupnění informací, které poskytuje přístup k veškerým datům v systému se závažným dopadem.	0,560

Tab. 10: Dopad integrity.

Hodnota	Popis	Skóre
Žádný (None – N)	Neexistuje žádný vliv na integritu systému.	0,000
Nízký (Low – L)	Modifikace některých dat nebo systémových souborů je možná, ale rozsah úpravy je omezen.	0,220
Vysoký (High – H)	Úplná ztráta integrity, útočník může modifikovat všechny soubory nebo informace v cílovém systému.	0,560

Tab. 11: Dopad dostupnosti.

Hodnota	Popis	Skóre
Žádný (None – N)	Neexistuje žádný vliv na dostupnost systému.	0,000
Nízký (Low – L)	Snížený výkon nebo ztráta některých funkcí.	0,220
Vysoký (High – H)	Úplná ztráta dostupnosti.	0,560

5.1.5 Určení míry rizika

Závěrečným krokem ve výpočtu je stanovení míry rizika, což je kombinace úrovně pravděpodobnosti výskytu rizika a úrovně zranitelnosti a dopadu. Konečná výše rizika je výsledkem vynásobené pravděpodobnosti výskytu hrozeb a jejich dopadu. Pro závěrečné porovnání jsem všechny hrozby a vypočtené hodnoty dosadil do společné tabulky.

5.1.6 Finanční dopad

Během analýzy rizik se určuje dopad i z pohledu finančního. Pokud jsou tyto informace známy, lze s nimi dále pracovat a využít je ke stanovení pravděpodobného finančního dopadu všech rizik, které v organizaci mohou nastat, Tento finanční dopad je vázaný na odhad pravděpodobnosti výskytu těchto rizik.

Vytvořil jsem Tab. **12** pro uvedení vzájemného vztahu faktorů následků (hodnota aktiva) a pravděpodobnosti výskytu hrozeb. Prvním krokem je ohodnocení aktiv (sloupec „b“ v tabulce), druhým krokem je vyhodnocení pravděpodobnosti výskytu hrozby (sloupec „c“ v tabulce). Třetím krokem je výpočet míry rizika násobením (b x c). Nakonec lze hrozby seřadit v pořadí podle výsledné míry rizika. Tento postup umožňuje srovnávat různé hrozby s rozdílnými následky a pravděpodobností výskytu a seřadit je podle priority.

Tab. 12: Výpočet finančního dopadu.

Popis hrozby (a)	Hodnota aktiv (b)	Pravděpodobnost výskytu hrozby (c)	Míra rizika (d)	Seřazení hrozeb (e)
Hrozba A				
Hrozba B				
Hrozba C				

5.1.7 Hodnocení rizika

Pro hodnocení rizika je nutné si stanovit škálu rizik a matici úrovní rizik pro vzájemné porovnání. Vytvořil jsem si matici, která je uvedena v Tab. **13**. Tato matice vyplývá z úvah o pravděpodobnosti výskytu rizika namapovaného proti vypočtenému dopadu. Tabulka propojuje pravděpodobnost s dopadem vztahujícím se k výskytu rizika. Výsledné riziko se měří na stupnici od 0 do 8 a může být vyhodnoceno podle kritérií akceptace rizika. Stupnice rizik je převedena do jednoduché škály rizik v Tab. **14**.

Tab. 13: Matice.

	Pravděpodobnost výskytu rizika	Velmi nízká	Nízká	Střední	Vysoká	Velmi vysoká
Dopad	Žádný	0	1	2	3	4
	Nízký	1	2	3	4	5
	Střední	2	3	4	5	6
	Vysoký	3	4	5	6	7
	Kritický	4	5	6	7	8

Tab. 14: Škála pravděpodobnosti a dopadu.

Pravděpodobnost výskytu		Dopad	
Velmi nízká	0 až 0,100	Žádný	0,0
Nízká	0,101 až 0,367	Nízký	0,1 až 3,9
Střední	0,368 až 0,634	Střední	4,0 až 6,9
Vysoká	0,635 až 0,899	Vysoký	7,0 až 8,9
Velmi vysoká	0,900 až 1,000	Kritický	9,0 až 10,0

5.2 QRA u zařízení průmyslový robot

V následujících kapitolách je proveden praktický výpočet u zařízení průmyslový robot. Provedeme výpočet pravděpodobnosti výskytu hrozby, zranitelnosti a dopadu, míry rizika a finančního dopadu. Na závěr je provedeno vyhodnocení analýzy rizika u tohoto zařízení.

5.2.1 Výpočet pravděpodobnosti výskytu hrozby

Analýza rizika začíná stanovením hrozeb a jejich faktorů, které jsou uvedeny v následujících tabulkách (Tab. **15**, Tab. **16**, Tab. **17**, Tab. **18**, Tab. **19**, Tab. **20**, Tab. **21**, Tab. **22** a Tab. **23**) s již stanovenými hodnotami optimistického, pesimistického pro-

centního výskytu, stanovením vah faktorů a vypočteným váženým aritmetickým průměrem dle vzorce **(5.1)**. Tabulky jsou rozděleny podle jednotlivých typů hrozeb.

Tab. 15: Pravděpodobnost výskytu hrozby vzdálená špionáž – robot.

Popis faktoru	P_{opt}	P_{pes}	Váha
Nedostatečně bezpečná síťová architektura	0,030	0,080	0,4
Přenos odkrytých hesel	0,008	0,015	0,3
Nechráněné komunikační linky	0,070	0,105	0,6
Nechráněné připojení do veřejné sítě	0,080	0,120	0,7
Vážený aritmetický průměr	0,056	0,112	
Aritmetický průměr	0,084		

Tab. 16: Pravděpodobnost výskytu hrozby nedůvěryhodná data – robot.

Popis faktoru	P_{opt}	P_{pes}	Váha
Nekontrolované stahování a užívání programů	0,200	0,260	0,8
Nedostatečné zálohování	0,025	0,090	0,4
Nedostatky ve formálním procesu pro autorizaci veřejně přístupných informací	0,100	0,350	0,1
Vážený aritmetický průměr	0,138	0,215	
Aritmetický průměr	0,177		

Tab. 17: Pravděpodobnost výskytu hrozby selhání zařízení – robot.

Popis faktoru	P_{opt}	P_{pes}	Váha
Nedostatečné bezpečnostní školení	0,050	0,090	0,3
Přehřátí zařízení	0,120	0,200	0,5
Chyba obsluhy	0,500	0,620	0,9
Neoprávněné použití	0,480	0,590	0,8
Vážený aritmetický průměr	0,364	0,463	
Aritmetický průměr	0,413		

Tab. 18: Pravděpodobnost výskytu hrozby chybné fungování zařízení – robot.

Popis faktoru	P_{opt}	P_{pes}	Váha
Nedostatečná dokumentace	0,070	0,120	0,3
Chyba obsluhy	0,510	0,550	0,9
Nedostatečně proškolená obsluha	0,450	0,520	0,7
Chybný software	0,200	0,260	0,4
Vážený aritmetický průměr	0,380	0,434	
Aritmetický průměr	0,407		

Tab. 19: Pravděpodobnost výskytu hrozby zneužití oprávnění – robot.

Popis faktoru	P_{opt}	P_{pes}	Váha
Nedostatečné testování programů	0,110	0,180	0,2
Známé chyby v programech	0,100	0,190	0,2
Neodhlášení se při opouštění pracovní stanice	0,340	0,420	0,8
Vážený aritmetický průměr	0,262	0,342	
Aritmetický průměr	0,302		

Tab. 20: Pravděpodobnost výskytu hrozby sociální inženýrství – robot.

Popis faktoru	P_{opt}	P_{pes}	Váha
Phishing – podvodný e-mail	0,350	0,480	0,5
Baiting – infikované médium	0,180	0,250	0,3
Sniffing – slídění	0,500	0,680	0,7
Malware – škodlivý software	0,700	0,790	0,8
Vážený aritmetický průměr	0,495	0,619	
Aritmetický průměr	0,557		

Tab. 21: Pravděpodobnost výskytu hrozby hackingu – robot.

Popis faktoru	P_{opt}	P_{pes}	Váha
Nedostatečně silná hesla	0,460	0,510	0,6
Slabina v systému	0,570	0,630	0,7
Nekontrolované kopírování	0,020	0,051	0,2
Vážený aritmetický průměr	0,453	0,505	
Aritmetický průměr	0,479		

Tab. 22: Pravděpodobnost výskytu hrozby škodlivý vir – robot.

Popis faktoru	P_{opt}	P_{pes}	Váha
Zneužití oprávnění	0,120	0,300	0,4
Nedostatečně silná hesla	0,470	0,580	0,9
Nekontrolované stahování a užívání programů	0,060	0,150	0,4
Nedostatek kontrolních mechanismů	0,007	0,013	0,1
Vážený aritmetický průměr	0,279	0,391	
Aritmetický průměr	0,335		

Tab. 23: Pravděpodobnost výskytu hrozby neoprávněný přístup – robot.

Popis faktoru	P_{opt}	P_{pes}	Váha
Nedostatečně silná hesla	0,330	0,450	0,9
Neúmyslné chyby a opomenutí	0,050	0,090	0,1
Chybné přiřazení přístupových práv	0,095	0,170	0,3
Neodhlášení se při opouštění pracovní stanice	0,300	0,525	0,8
Vážený aritmetický průměr	0,272	0,421	
Aritmetický průměr	0,347		

5.2.2 Výpočet zranitelnosti a dopadu

Dalším krokem je výpočet zranitelnosti a dopadu. Dle metodiky CVSS jsem vytvořil tabulky pro jednotlivé hrozby a dle online kalkulátoru jsem dosadil a vypočítal základní skóre hodnoty zranitelnosti a dopadu. Výsledné základní skóre je vypočteno podle vzorců **(5.3)** a **(5.4)**. U každé hrozby jsou popsány jednotlivé hodnoty v Tab. **24**, Tab. **25**, Tab. **26**, Tab. **27**, Tab. **28**, Tab. **29**, Tab. **30**, Tab. **31** a Tab. **32**.

Tab. 24: Zranitelnost a dopad vzdálené špionáže – robot.

Metrika	Hodnota	Popis	Skóre
Přístupový vektor	Síť (Network – N)	Útočník se připojí k využitelné databázi MySQL prostřednictvím sítě.	0,850
Složitost útoku	Nízký (Low – L)	Neexistují žádné zvláštní podmínky pro zneužití.	0,770
Požadovaná oprávnění	Nízký (Low – L)	Útočník má oprávnění, která poskytují základní uživatelské funkce.	0,620
Interakce uživatele	Žádný (None – N)	Citlivý systém může být využíván bez interakce uživatele.	0,850
Rozsah	Změna (Changed – C)	Útok může ovlivnit i prostředky s vyšším oprávněním.	0,752
Dopad důvěrnosti	Nízký (Low – L)	Rozsah ztráty je omezen, ne všechny údaje jsou k dispozici.	0,220
Dopad integrity	Nízký (Low – L)	Rozsah úpravy souboru je omezen.	0,220
Dopad dostupnosti	Žádný (None – N)	Neexistuje žádný vliv na dostupnost systému.	0,000
Výsledné základní skóre			6,400

Tab. 25: Zranitelnost a dopad nedůvěryhodných dat – robot.

Metrika	Hodnota	Popis	Skóre
Přístupový vektor	Místní (Local – L)	Vzdálený uživatel vytvořil speciální soubor, který při načtení spustí chybu.	0,550
Složitost útoku	Nízký (Low – L)	Specializované podmínky nejsou vyžadovány.	0,770
Požadovaná oprávnění	Žádný (None – N)	Nevyžaduje žádný přístup k provedení útoku.	0,850
Interakce uživatele	Požadovaný (Required – R)	Útočník musí přesvědčit uživatele, aby otevřel škodlivý soubor.	0,620
Rozsah	Beze změny (Unchanged – U)	Útok může ovlivnit pouze prostředky spravované stejným oprávněním.	0,642
Dopad důvěrnosti	Vysoký (High – H)	Úplná ztráta důvěrnosti.	0,560
Dopad integrity	Vysoký (High – H)	Úplná ztráta integrity.	0,560
Dopad dostupnosti	Vysoký (High – H)	Úplná ztráta dostupnosti.	0,560
Výsledné základní skóre			7,800

Tab. 26: Zranitelnost a dopad selhání zařízení – robot.

Metrika	Hodnota	Popis	Skóre
Přístupový vektor	Místní (Local – L)	Útok umožňuje využít jiný analyzátor XML.	0,550
Složitost útoku	Nízký (Low – L)	Neexistují žádné zvláštní podmínky pro zneužití.	0,770
Požadovaná oprávnění	Vysoký (High – H)	Útočník má administrativní kontrolu.	0,270
Interakce uživatele	Žádný (None – N)	Systém bez interakce uživatele.	0,850
Rozsah	Beze změny (Unchanged – U)	Útok může ovlivnit pouze prostředky spravované stejným oprávněním.	0,642
Dopad důvěrnosti	Nízký (Low – L)	Rozsah ztráty je omezen, ne všechny údaje jsou k dispozici.	0,220
Dopad integrity	Nízký (Low – L)	Rozsah úpravy souboru je omezen.	0,220
Dopad dostupnosti	Nízký (Low – L)	Snížený výkon nebo ztráta některých funkcí.	0,220
Výsledné základní skóre			4,200

Tab. 27: Zranitelnost a dopad chybného fungování zařízení – robot.

Metrika	Hodnota	Popis	Skóre
Přístupový vektor	Síť (Network – N)	Při návštěvě webového serveru útočník změní síťový provoz mezi obětí a serverem.	0,850
Složitost útoku	Vysoká (High – H)	Existují speciální požadavky na metody sociálního inženýrství.	0,440
Požadovaná oprávnění	Žádný (None – N)	Útočník nevyžaduje přístup k provedení útoku.	0,850
Interakce uživatele	Požadovaný (Required – R)	Je nutná interakce uživatele.	0,620
Rozsah	Beze změny (Unchanged – U)	Útok ovlivňuje pouze prostředky se stejným oprávněním.	0,642
Dopad důvěrnosti	Nízký (Low – L)	Rozsah ztrát je omezen.	0,220
Dopad integrity	Žádný (None – N)	Neexistuje vliv na integritu systému.	0,000
Dopad dostupnosti	Žádný (None – N)	Neexistuje vliv na dostupnost systému.	0,000
Výsledné základní skóre			3,100

Tab. 28: Zranitelnost a dopad zneužití oprávnění – robot.

Metrika	Hodnota	Popis	Skóre
Přístupový vektor	Místní (Local – L)	Útok umožňuje vzdáleným útočníkům provádět změnu kódu.	0,550
Složitost útoku	Nízký (Low – L)	Neexistují žádné zvláštní podmínky pro zneužití.	0,770
Požadovaná oprávnění	Žádný (None – N)	Útočník nevyžaduje přístup k provedení útoku.	0,850
Interakce uživatele	Požadovaný (Required – R)	Je nutná interakce uživatele.	0,620
Rozsah	Beze změny (Unchanged – U)	Útok ovlivňuje pouze prostředky se stejným oprávněním.	0,642
Dopad důvěrnosti	Vysoká (High – H)	Úplná ztráta důvěrnosti.	0,560
Dopad integrity	Vysoká (High – H)	Úplná ztráta integrity.	0,560
Dopad dostupnosti	Vysoká (High – H)	Úplná ztráta dostupnosti.	0,560
Výsledné základní skóre			7,800

Tab. 29: Zranitelnost a dopad sociálního inženýrství – robot.

Metrika	Hodnota	Popis	Skóre
Přístupový vektor	Síť (Network – N)	Útočník musí přesvědčit uživatele o otevření škodlivého souboru.	0,850
Složitost útoku	Nízký (Low – L)	Neexistují žádné zvláštní podmínky pro zneužití.	0,770
Požadovaná oprávnění	Nízký (Low – L)	Útočník má oprávnění, která poskytují základní uživatelské funkce.	0,620
Interakce uživatele	Žádný (None – N)	Systém bez interakce uživatele.	0,850
Rozsah	Beze změny (Unchanged – U)	Útok ovlivňuje pouze prostředky se stejným oprávněním.	0,642
Dopad důvěrnosti	Vysoká (High – H)	Úplná ztráta důvěrnosti.	0,560
Dopad integrity	Vysoká (High – H)	Úplná ztráta integrity.	0,560
Dopad dostupnosti	Vysoká (High – H)	Úplná ztráta dostupnosti.	0,560
Výsledné základní skóre			8,800

Tab. 30: Zranitelnost a dopad hackingu – robot.

Metrika	Hodnota	Popis	Skóre
Přístupový vektor	Místní (Local – L)	Útočník musí oběti doručit škodlivý dokument a spoléhat na jeho otevření.	0,550
Složitost útoku	Nízký (Low – L)	Neexistují žádné zvláštní podmínky pro zneužití.	0,770
Požadovaná oprávnění	Žádný (None – N)	Útočník nevyžaduje přístup k provedení útoku.	0,850
Interakce uživatele	Požadovaný (Required – R)	Je nutná interakce uživatele.	0,620
Rozsah	Beze změny (Unchanged – U)	Útok ovlivňuje pouze prostředky se stejným oprávněním.	0,642
Dopad důvěrnosti	Vysoká (High – H)	Úplná ztráta důvěrnosti.	0,560
Dopad integrity	Vysoká (High – H)	Úplná ztráta integrity.	0,560
Dopad dostupnosti	Vysoká (High – H)	Úplná ztráta dostupnosti.	0,560
Výsledné základní skóre			7,800

Tab. 31: Zranitelnost a dopad škodlivého viru – robot.

Metrika	Hodnota	Popis	Skóre
Přístupový vektor	Síť (Network – N)	Útočník doručí oběti dokument obsahující škodlivý vir.	0,850
Složitost útoku	Nízký (Low – L)	Neexistují žádné zvláštní podmínky pro zneužití.	0,770
Požadovaná oprávnění	Žádný (None – N)	Útočník nevyžaduje přístup k provedení útoku.	0,850
Interakce uživatele	Žádný (None – N)	Systém bez interakce uživatele.	0,850
Rozsah	Beze změny (Unchanged – U)	Útok ovlivňuje pouze prostředky se stejným oprávněním.	0,642
Dopad důvěrnosti	Vysoká (High – H)	Úplná ztráta důvěrnosti.	0,560
Dopad integrity	Žádný (None – N)	Neexistuje vliv na integritu systému.	0,000
Dopad dostupnosti	Žádný (None – N)	Neexistuje vliv na dostupnost systému.	0,000
Výsledné základní skóre			7,500

Tab. 32: Zranitelnost a dopad neoprávněného přístupu do systému – robot.

Metrika	Hodnota	Popis	Skóre
Přístupový vektor	Síť (Network – N)	Vrácená data obsahují citlivé informace, které útočník použije k zahájení dalších útoků.	0,850
Složitost útoku	Vysoká (High – H)	Existují speciální podmínky a požadavky.	0,440
Požadovaná oprávnění	Žádný (None – N)	Útočník nevyžaduje přístup k provedení útoku.	0,850
Interakce uživatele	Žádný (None – N)	Systém bez interakce uživatele.	0,850
Rozsah	Změna (Changed – C)	Útok může ovlivnit i prostředky s vyšším oprávněním.	0,752
Dopad důvěrnosti	Žádný (None – N)	Neexistuje vliv na důvěrnost systému.	0,000
Dopad integrity	Vysoká (High – H)	Úplná ztráta integrity.	0,560
Dopad dostupnosti	Žádný (None – N)	Neexistuje vliv na dostupnost systému.	0,000
Výsledné základní skóre			6,800

5.2.3 Výpočet míry rizika

Závěrečným krokem ve výpočtu je stanovení míry rizika, což je kombinace úrovně pravděpodobnosti výskytu hrozby a úrovně dopadu. V Tab. **33** jsou dosazeny hodnoty pravděpodobnosti výskytu a hodnoty dopadu. Pronásobením těchto dvou hodnot je vypočteno výsledné riziko.

Tab. 33: Výpočet míry rizika.

Typ	Hrozby	Pravděpodobnost	Dopad	Riziko
Ohrožení informací	Vzdálená špionáž	0,084	6,400	0,538
	Data pocházející z nedůvěryhodných zdrojů	0,177	7,800	1,381
	Selhání zařízení	0,413	4,200	1,735
	Chybné fungování zařízení	0,407	3,100	1,262
Ohrožení z kyberprostoru	Zneužití oprávnění	0,302	7,800	2,356
	Sociální inženýrství	0,557	8,800	4,902
	Hacking	0,479	7,800	3,736
	Škodlivý virus	0,335	7,500	2,513
	Neoprávněný přístup do systému	0,347	6,800	2,360

5.2.4 Výpočet finančního dopadu

Pro určení finančního dopadu je nutné stanovit hodnotu aktiv, které mohou být ohroženy hrozbami. Hodnota zařízení průmyslový robot se pohybuje v rozmezí 700 000 Kč až 1 000 000 Kč [31]. Hodnota aktiva výrobního procesu je stanovena finanční ztrátou, která nastane v případě útoku na zařízení. Hodnota ostatních aktiv, jako jsou operační systém, specifická podniková aplikace, komunikační rozhraní a operační paměť, je stanovena v hodnotě 100 000 Kč [31]. U hrozeb máme již vypočtenou pravděpodobnost výskytu hrozby, kterou dosadíme do následující Tab. **34**. Vynásobením hodnoty aktiva pravděpodobnosti výskytu hrozby dostaneme míru rizika, kterou doplníme do sloupce (d). Jednotlivé hrozbám na závěr přiřadíme dosažené pořadí.

Tab. 34: Výpočet finančního dopadu – průmyslový robot.

Popis hrozby (a)	Hodnota aktiv (b)	Pravděpodobnost výskytu hrozby (c)	Míra rizika (d)	Seřazení hrozeb (e)
Vzdálená špionáž	400 000 Kč	0,084	33 600 Kč	8.
Data pocházející z nedůvěryhodných zdrojů	150 000 Kč	0,177	26 550 Kč	9.
Selhání zařízení	650 000 Kč	0,413	268 450 Kč	3.
Chybné fungování zařízení	500 000 Kč	0,407	203 500 Kč	4.
Zneužití oprávnění	500 000 Kč	0,302	151 000 Kč	5.
Sociální inženýrství	700 000 Kč	0,557	389 900 Kč	1.
Hacking	600 000 Kč	0,479	287 400 Kč	2.
Škodlivý virus	380 000 Kč	0,335	127 300 Kč	6.
Neoprávněný přístup do systému	200 000 Kč	0,347	69 400 Kč	7.

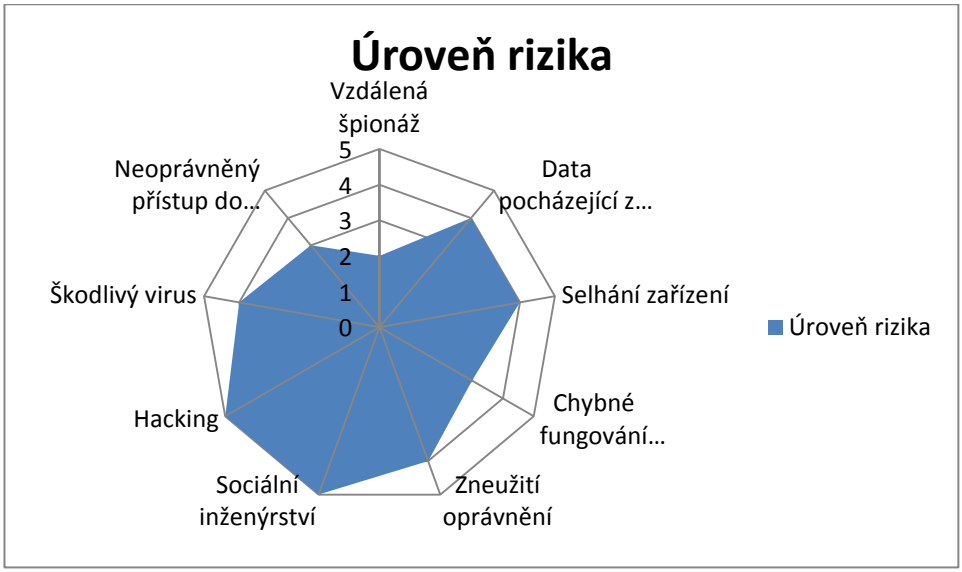
5.2.5 Hodnocení míry rizika

Dle Tab. **13** a Tab. **14** jsem vypočtené hodnoty míry rizika převedl podle předem stanovené matice na hodnoty úrovně jednotlivých rizik, které se mohou vzájemně porovnat, a tyto hodnoty vložil do Tab. **35.** Na základě vypočítaných hodnot u tohoto zařízení lze vyvodit, že ani jedno z rizik nespadá do kategorie nepřijatelných rizik a tedy nevyžaduje neodkladné zavedení protiopatření ke snížení rizika. U dvou hrozeb byla dosažena úroveň s hodnotou 5 a to u hrozby sociální inženýrství a hacking. Tyto dvě hrozby znamenají nebezpečí z hlediska kybernetického útoku. Tato dosažená úroveň není příznivá, je nutné ji monitorovat a případně přijmout opatření k jejímu snížení. Naopak u hrozby vzdálená špionáž byla dosažena úroveň s hodnotou 2, jedná se tedy o přijatelné riziko u zkoumaného zařízení.

Tab. 35: Úrovně rizika u zařízení průmyslový robot.

Typ	Hrozby	Úroveň rizika
Ohrožení informací	Vzdálená špionáž	2
	Data pocházející z nedůvěryhodných zdrojů	4
	Selhání zařízení	4
	Chybné fungování zařízení	3
Ohrožení z kyberprostoru	Zneužití oprávnění	4
	Sociální inženýrství	5
	Hacking	5
	Škodlivý virus	4
	Neoprávněný přístup do systému	3

Pro větší přehlednost jsem výsledné hodnoty úrovně rizika vložil do následujícího paprskového grafu s názvem Úroveň rizika u zařízení průmyslový robot (Obr. 4).



Obr. 4: Graf – úroveň rizika u zařízení průmyslový robot.

5.3 QRA u zařízení infuzní pumpa

V následujících kapitolách je proveden praktický výpočet u zařízení infuzní pumpa. Provedeme výpočet pravděpodobnosti výskytu hrozby, dopadu, míry rizika a finančního dopadu. Na závěr je provedeno vyhodnocení analýzy rizika u tohoto zařízení.

5.3.1 Výpočet pravděpodobnosti výskytu hrozby

Analýza rizika u zařízení infuzní pumpa začíná stanovením hrozeb a jejich faktorů, které jsou uvedeny v následujících tabulkách (Tab. **36**, Tab. **37**, Tab. **38**, Tab. **39**, Tab. **40**, Tab. **41**, Tab. **42**, Tab. **43** a Tab. **44**) s již stanovenými hodnotami optimistického, pesimistického procentního výskytu, stanovením vah faktorů a vypočteným váženým aritmetickým průměrem dle vzorce **(5.2)**.

Tab. 36: Pravděpodobnost výskytu hrozby vzdálená špionáž – pumpa.

Popis faktoru	P_{opt}	P_{pes}	Váha
Nedostatečně bezpečná síťová architektura	0,030	0,120	0,4
Přenos odkrytých hesel	0,008	0,150	0,3
Nechráněné komunikační linky	0,070	0,135	0,6
Nechráněné připojení do veřejné	0,080	0,170	0,7
Vážený aritmetický průměr	0,056	0,147	
Aritmetický průměr	0,101		

Tab. 37: Pravděpodobnost výskytu hrozby nedůvěryhodná data – pumpa.

Popis faktoru	P_{opt}	P_{pes}	Váha
Nekontrované stahování a užívání programů	0,040	0,080	0,8
Nedostatečné zálohování	0,025	0,050	0,4
Nedostatky ve formálním procesu pro autorizaci veřejně přístupných informací	0,010	0,300	0,1
Vážený aritmetický průměr	0,033	0,088	
Aritmetický průměr	0,060		

Tab. 38: Pravděpodobnost výskytu hrozby selhání zařízení – pumpa.

Popis faktoru	P_{opt}	P_{pes}	Váha
Nedostatečné bezpečnostní školení	0,050	0,090	0,3
Přehřátí zařízení	0,120	0,200	0,5
Chyba obsluhy	0,490	0,620	0,9
Neoprávněné použití	0,500	0,630	0,8
Vážený aritmetický průměr	0,366	0,476	
Aritmetický průměr	0,421		

Tab. 39: Pravděpodobnost výskytu hrozby chybné fungování zařízení – pumpa.

Popis faktoru	P_{opt}	P_{pes}	Váha
Nedostatečná dokumentace	0,070	0,120	0,3
Chyba obsluhy	0,460	0,530	0,9
Nedostatečně proškolená obsluha	0,300	0,420	0,7
Chybný software	0,120	0,210	0,4
Vážený aritmetický průměr	0,301	0,387	
Aritmetický průměr	0,344		

Tab. 40: Pravděpodobnost výskytu hrozby zneužití oprávnění – pumpa.

Popis faktoru	P_{opt}	P_{pes}	Váha
Nedostatečné testování programů	0,008	0,013	0,2
Známé chyby v programech	0,004	0,009	0,2
Neodhlášení se při opouštění pracovní stanice	0,050	0,100	0,8
Vážený aritmetický průměr	0,035	0,070	
Aritmetický průměr	0,050		

Tab. 41: Pravděpodobnost výskytu hrozby sociální inženýrství – pumpa.

Popis faktoru	P_{opt}	P_{pes}	Váha
Phishing – podvodný e-mail	0,007	0,013	0,5
Baiting – infikované médium	0,003	0,007	0,3
Sniffing – slídění	0,012	0,016	0,7
Malware – škodlivý software	0,011	0,017	0,8
Vážený aritmetický průměr	0,009	0,015	
Aritmetický průměr	0,012		

Tab. 42: Pravděpodobnost výskytu hrozby hackingu – pumpa.

Popis faktoru	P_{opt}	P_{pes}	Váha
Nedostatečně silná hesla	0,020	0,050	0,6
Slabina v systému	0,040	0,080	0,7
Nekontrolované kopírování	0,001	0,004	0,2
Vážený aritmetický průměr	0,027	0,058	
Aritmetický průměr	0,042		

Tab. 43: Pravděpodobnost výskytu hrozby škodlivý vir – pumpa.

Popis faktoru	P_{opt}	P_{pes}	Váha
Zneužití oprávnění	0,020	0,040	0,4
Nedostatečně silná hesla	0,040	0,060	0,9
Nekontrolované stahování a užívání programů	0,004	0,009	0,4
Nedostatek kontrolních mechanizmů	0,007	0,013	0,1
Vážený aritmetický průměr	0,026	0,042	
Aritmetický průměr	0,034		

Tab. 44: Pravděpodobnost výskytu hrozby neoprávněný přístup – pumpa.

Popis faktoru	P_{opt}	P_{pes}	Váha
Nedostatečně silná hesla	0,030	0,070	0,9
Neúmyslné chyby a opomenutí	0,002	0,005	0,1
Chybné přiřazení přístupových práv	0,050	0,080	0,3
Neodhlášení se při opouštění pracovní stanice	0,240	0,350	0,8
Vážený aritmetický průměr	0,112	0,175	
Aritmetický průměr	0,143		

5.3.2 Výpočet zranitelnosti a dopadu

Dalším krokem je výpočet zranitelnosti a dopadu. Dle metodiky CVSS jsem vytvořil tabulky pro jednotlivé hrozby a dle online kalkulátoru jsem dosadil a vypočítal základní skóre hodnoty zranitelnosti a dopadu. Výsledné základní skóre je vypočteno podle vzorce **(5.3)** a **(5.4)**. U každé hrozby jsou popsány jednotlivé hodnoty a vloženy do Tab. **45**, Tab. **46**, Tab. **47**, Tab. **48**, Tab. **49**, Tab. **50**, Tab. **51**, Tab. **52** a Tab. **53**.

Tab. 45: Zranitelnost a dopad vzdálené špionáže – pumpa.

Metrika	Hodnota	Popis	Skóre
Přístupový vektor	Místní (Local – L)	Útočník má buď fyzický přístup, nebo lokální účet.	0,550
Složitost útoku	Vysoký (High – H)	Existují speciální požadavky na metody sociálního inženýrství.	0,440
Požadovaná oprávnění	Nízký (Low – L)	Útočník má oprávnění, která poskytují základní uživatelské funkce.	0,620
Interakce uživatele	Žádný (None – N)	Citlivý systém může být využíván bez interakce uživatele.	0,850
Rozsah	Změna (Changed – C)	Útok může ovlivnit i prostředky s vyšším oprávněním.	0,752
Dopad důvěrnosti	Nízký (Low – L)	Rozsah ztráty je omezen, ne všechny údaje jsou k dispozici.	0,220
Dopad integrity	Nízký (Low – L)	Rozsah úpravy souboru je omezen.	0,220
Dopad dostupnosti	Žádný (None – N)	Neexistuje žádný vliv na dostupnost systému.	0,000
Výsledné základní skóre			4,200

Tab. 46: Zranitelnost a dopad nedůvěryhodných dat – pumpa.

Metrika	Hodnota	Popis	Skóre
Přístupový vektor	Fyzický (Physical – P)	Útočník musí mít fyzický přístup k zařízení.	0,200
Složitost útoku	Nízký (Low – L)	Specializované podmínky nejsou vyžadovány.	0,770
Požadovaná oprávnění	Žádný (None – N)	Nevyžaduje žádný přístup k provedení útoku.	0,850
Interakce uživatele	Požadovaný (Required – R)	Útočník musí přesvědčit uživatele, aby otevřel škodlivý soubor.	0,620
Rozsah	Beze změny (Unchanged – U)	Útok může ovlivnit pouze prostředky spravované stejným oprávněním.	0,642
Dopad důvěrnosti	Vysoký (High – H)	Úplná ztráta důvěrnosti.	0,560
Dopad integrity	Vysoký (High – H)	Úplná ztráta integrity.	0,560
Dopad dostupnosti	Vysoký (High – H)	Úplná ztráta dostupnosti.	0,560
Výsledné základní skóre			6,600

Tab. 47: Zranitelnost a dopad selhání zařízení – pumpa.

Metrika	Hodnota	Popis	Skóre
Přístupový vektor	Místní (Local – L)	Útočník má buď fyzický přístup, nebo lokální účet.	0,550
Složitost útoku	Nízký (Low – L)	Neexistují žádné zvláštní podmínky pro zneužití.	0,770
Požadovaná oprávnění	Vysoký (High – H)	Útočník má administrativní kontrolu.	0,270
Interakce uživatele	Žádný (None – N)	Systém bez interakce uživatele.	0,850
Rozsah	Beze změny (Unchanged – U)	Útok může ovlivnit pouze prostředky spravované stejným oprávněním.	0,642
Dopad důvěrnosti	Nízký (Low – L)	Rozsah ztráty je omezen, ne všechny údaje jsou k dispozici.	0,220
Dopad integrity	Nízký (Low – L)	Rozsah úpravy souboru je omezen.	0,220
Dopad dostupnosti	Vysoký (High – H)	Úplná ztráta dostupnosti.	0,560
Výsledné základní skóre			5,600

Tab. 48: Zranitelnost a dopad chybného fungování zařízení – pumpa.

Metrika	Hodnota	Popis	Skóre
Přístupový vektor	Místní (Local – L)	Útočník má buď fyzický přístup, nebo lokální účet.	0,550
Složitost útoku	Vysoká (High – H)	Existují speciální požadavky na metody sociálního inženýrství.	0,440
Požadovaná oprávnění	Žádný (None – N)	Útočník nevyžaduje přístup k provedení útoku.	0,850
Interakce uživatele	Požadovaný (Required – R)	Je nutná interakce uživatele.	0,620
Rozsah	Beze změny (Unchanged – U)	Útok ovlivňuje pouze prostředky se stejným oprávněním.	0,642
Dopad důvěrnosti	Nízký (Low – L)	Rozsah ztrát informací je omezen.	0,220
Dopad integrity	Nízký (Low – L)	Rozsah úpravy souboru je omezen	0,220
Dopad dostupnosti	Vysoký (High – H)	Úplná ztráta dostupnosti.	0,560
Výsledné základní skóre			5,800

Tab. 49: Zranitelnost a dopad zneužití oprávnění – pumpa.

Metrika	Hodnota	Popis	Skóre
Přístupový vektor	Fyzický (Physical – P)	Útočník musí mít fyzický přístup k zařízení.	0,200
Složitost útoku	Vysoká (High – H)	Existují speciální požadavky na metody sociálního inženýrství.	0,440
Požadovaná oprávnění	Žádný (None – N)	Útočník nevyžaduje přístup k provedení útoku.	0,850
Interakce uživatele	Požadovaný (Required – R)	Je nutná interakce uživatele.	0,620
Rozsah	Beze změny (Unchanged – U)	Útok ovlivňuje pouze prostředky se stejným oprávněním.	0,642
Dopad důvěrnosti	Vysoká (High – H)	Úplná ztráta důvěrnosti.	0,560
Dopad integrity	Nízký (Low – L)	Rozsah úpravy souboru je omezen	0,560
Dopad dostupnosti	Vysoká (High – H)	Úplná ztráta dostupnosti.	0,560
Výsledné základní skóre			5,900

Tab. 50: Zranitelnost a dopad sociálního inženýrství – pumpa.

Metrika	Hodnota	Popis	Skóre
Přístupový vektor	Fyzický (Physical – P)	Útočník musí mít fyzický přístup k zařízení.	0,200
Složitost útoku	Nízký (Low – L)	Neexistují žádné zvláštní podmínky pro zneužití.	0,770
Požadovaná oprávnění	Nízký (Low – L)	Útočník má oprávnění, která poskytují základní uživatelské funkce.	0,620
Interakce uživatele	Žádný (None – N)	Systém bez interakce uživatele.	0,850
Rozsah	Změna (Changed – C)	Útok může ovlivnit i prostředky s vyšším oprávněním.	0,752
Dopad důvěrnosti	Vysoká (High – H)	Úplná ztráta důvěrnosti.	0,560
Dopad integrity	Vysoká (High – H)	Úplná ztráta integrity.	0,560
Dopad dostupnosti	Vysoká (High – H)	Úplná ztráta dostupnosti.	0,560
Výsledné základní skóre			7,400

Tab. 51: Zranitelnost a dopad hackingu – pumpa.

Metrika	Hodnota	Popis	Skóre
Přístupový vektor	Místní (Local – L)	Útočník má buď fyzický přístup, nebo lokální účet.	0,550
Složitost útoku	Nízký (Low – L)	Neexistují žádné zvláštní podmínky pro zneužití.	0,770
Požadovaná oprávnění	Žádný (None – N)	Útočník nevyžaduje přístup k provedení útoku.	0,850
Interakce uživatele	Požadovaný (Required – R)	Je nutná interakce uživatele.	0,620
Rozsah	Beze změny (Unchanged – U)	Útok ovlivňuje pouze prostředky se stejným oprávněním.	0,642
Dopad důvěrnosti	Vysoká (High – H)	Úplná ztráta důvěrnosti.	0,560
Dopad integrity	Vysoká (High – H)	Úplná ztráta integrity.	0,560
Dopad dostupnosti	Vysoká (High – H)	Úplná ztráta dostupnosti.	0,560
Výsledné základní skóre			7,800

Tab. 52: Zranitelnost a dopad škodlivého viru – pumpa.

Metrika	Hodnota	Popis	Skóre
Přístupový vektor	Místní (Local – L)	Útočník má buď fyzický přístup, nebo lokální účet.	0,550
Složitost útoku	Nízký (Low – L)	Neexistují žádné zvláštní podmínky pro zneužití.	0,770
Požadovaná oprávnění	Žádný (None – N)	Útočník nevyžaduje přístup k provedení útoku.	0,850
Interakce uživatele	Žádný (None – N)	Systém bez interakce uživatele.	0,850
Rozsah	Beze změny (Unchanged – U)	Útok ovlivňuje pouze prostředky se stejným oprávněním.	0,642
Dopad důvěrnosti	Vysoká (High – H)	Úplná ztráta důvěrnosti.	0,560
Dopad integrity	Žádný (None – N)	Neexistuje vliv na integritu systému.	0,000
Dopad dostupnosti	Žádný (None – N)	Neexistuje vliv na dostupnost systému.	0,000
Výsledné základní skóre			6,200

Tab. 53: Zranitelnost a dopad neoprávněného přístupu do systému – pumpa.

Metrika	Hodnota	Popis	Skóre
Přístupový vektor	Fyzický (Physical – P)	Útočník musí mít fyzický přístup k zařízení.	0,200
Složitost útoku	Vysoká (High – H)	Existují speciální podmínky a požadavky.	0,440
Požadovaná oprávnění	Žádný (None – N)	Útočník nevyžaduje přístup k provedení útoku.	0,850
Interakce uživatele	Žádný (None – N)	Systém bez interakce uživatele.	0,850
Rozsah	Změna (Changed – C)	Útok může ovlivnit i prostředky s vyšším oprávněním.	0,752
Dopad důvěrnosti	Vysoká (High – H)	Úplná ztráta důvěrnosti.	0,560
Dopad integrity	Vysoká (High – H)	Úplná ztráta integrity.	0,560
Dopad dostupnosti	Vysoká (High – H)	Úplná ztráta dostupnosti.	0,560
Výsledné základní skóre			7,100

5.3.3 Výpočet míry rizika

Závěrečným krokem ve výpočtu je stanovení míry rizika, což je kombinace úrovně pravděpodobnosti výskytu hrozby a úrovně dopadu. V Tab. **54** jsou dosazeny hodnoty pravděpodobnosti výskytu, dále hodnoty dopadu. Pronásobením těchto dvou hodnot je vypočteno výsledné riziko.

Tab. 54: Výpočet míry rizika.

Typ	Hrozby	Pravděpodobnost	Dopad	Riziko
Ohrožení informací	Vzdálená špionáž	0,101	4,200	0,424
	Data pocházející z nedůvěryhodných zdrojů	0,060	6,600	0,396
	Selhání zařízení	0,421	5,600	2,358
	Chybné fungování zařízení	0,344	5,800	1,996
Ohrožení z kyberprostoru	Zneužití oprávnění	0,050	5,900	0,295
	Sociální inženýrství	0,012	7,400	0,089
	Hacking	0,042	7,800	0,328
	Škodlivý virus	0,034	6,200	0,211
	Neoprávněný přístup do systému	0,143	7,100	1,015

5.3.4 Výpočet finančního dopadu

Pro určení finančního dopadu je nutné stanovit hodnotu aktiv, které mohou být ohroženy hrozbami. Hodnota zařízení infuzní pumpa se pohybuje v rozmezí 15 000 Kč až 40 000 Kč [30]. Hodnota ostatních aktiv, jako jsou hardware, operační systém a specifický software, je stanovena v hodnotě 30 000 Kč [30]. U hrozeb máme již vypočtenou pravděpodobnost výskytu hrozby, kterou dosadíme do následující Tab. **55**. Vynásobením hodnoty aktiva pravděpodobnosti výskytu hrozby dostaneme míru rizika, kterou doplníme do sloupce (d). Jednotlivé hrozbám na závěr přiřadíme dosažené pořadí.

Tab. 55: Výpočet finančního dopadu – infuzní pumpa.

Popis hrozby (a)	Hodnota aktiv (b)	Pravděpodobnost výskytu hrozby (c)	Míra rizika (d)	Seřazení hrozeb (e)
Vzdálená špionáž	20 000 Kč	0,101	2 020 Kč	5.
Data pocházející z nedůvěryhodných zdrojů	15 000 Kč	0,060	900 Kč	8.
Selhání zařízení	250 000 Kč	0,421	105 250 Kč	1.
Chybné fungování zařízení	150 000 Kč	0,344	51 600 Kč	2.
Zneužití oprávnění	20 000 Kč	0,050	1 000 Kč	6.
Sociální inženýrství	78 000 Kč	0,012	936 Kč	7.
Hacking	60 000 Kč	0,042	2 520 Kč	4.
Škodlivý virus	18 000 Kč	0,034	612 Kč	9.
Neoprávněný přístup do systému	22 000 Kč	0,143	3 146 Kč	3.

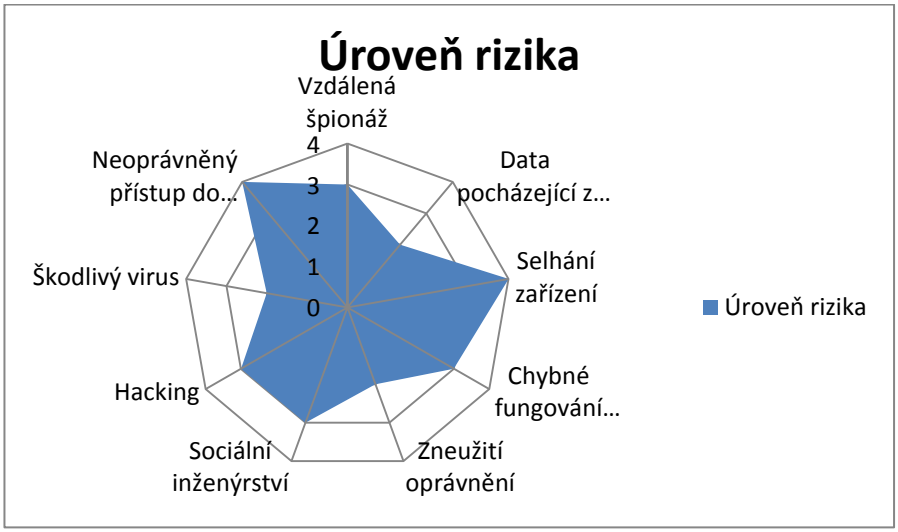
5.3.5 Hodnocení míry rizika

Stejně jako u předcházejícího zařízení, i zde jsem vypočtené hodnoty míry rizika dle Tab. **13** a Tab. **14** převedl podle předem stanovené matice na hodnoty úrovně jednotlivých rizik, které se mohou vzájemně porovnat, a tyto hodnoty vložil do Tab. **56**. Na základě vypočítaných hodnot u tohoto zařízení lze vyvodit, že ani jedno z rizik nespadá do kategorie nepřijatelných rizik a tedy nevyžaduje neodkladné zavedení protiopatření ke snížení rizika. U dvou hrozeb byla dosažena nejvyšší úroveň s hodnotou 4 a to u hrozby selhání zařízení a neoprávněný přístup do systému. Tyto dvě hrozby u tohoto zařízení mají nebezpečný charakter, mohou negativně ovlivnit bezpečnost pacienta. Tato dosažená úroveň není příznivá, je nutné ji monitorovat a případně přijmout opatření k jejímu snížení. Naopak u hrozeb data pocházející z nedůvěryhodných zdrojů, zneužití oprávnění, a škodlivý virus byla dosažena úroveň s hodnotou 2, jedná se tedy o zanedbatelné riziko u zkoumaného zařízení. Toto zařízení je těžko napadnutelné v kyberprostoru, neboť k němu má přístup pouze omezený počet osob a není připojeno k veřejné počítačové síti, přesto jakákoliv sebemenší hrozba může mít fatální následky.

Tab. 56: Úrovně rizika u zařízení infuzní pumpa.

Typ	Hrozby	Úroveň rizika
Ohrožení informací	Vzdálená špionáž	3
	Data pocházející z nedůvěryhodných zdrojů	2
	Selhání zařízení	4
	Chybné fungování zařízení	3
Ohrožení z kyberprostoru	Zneužití oprávnění	2
	Sociální inženýrství	3
	Hacking	3
	Škodlivý virus	2
	Neoprávněný přístup do systému	4

Pro větší přehlednost jsem výsledné hodnoty úrovně rizika vložil do následujícího paprskového grafu s názvem Úroveň rizika u zařízení infuzní pumpa (Obr. 5).



Obr. 5: Graf – úroveň rizika u zařízení infuzní pumpa.

6. Závěr

Tato bakalářská práce byla věnována kvantitativnímu přístupu k rizikové analýze v rámci kybernetické bezpečnosti.

V teoretické části byly, pro lepší pochopení problematiky, definovány pojmy týkající se dané problematiky a popsány různé metody. Byl vymezen pojem kybernetická bezpečnost, kybernetický prostor a jeho pojetí, kybernetický incident a krize. Dále byla srovnána kybernetická a informační bezpečnost. Proces řízení rizik dle normy ISO/IEC 27005 byl podrobně představen a rozebrán a s ním i metodika NIST. Riziková analýza se dělí na tři metody – kvalitativní, kvantitativní a semikvantitativní. V této bakalářské práci byla použita kvantitativní riziková analýza. Tyto metody byly vzájemně porovnány a jejich výhody a nevýhody byly seřazeny přehledně do tabulky. Závěrem teoretické části byly uvedeny příklady kvantitativní metod a představena triáda CIA s vysvětlením pojmů.

Druhá část této bakalářské práce byla věnována vypracování QRA metody. Nejdříve jsem vybral dvě zařízení a to průmyslový robot a infuzní pumpa. Metodu jsem nejdříve popsal obecně po jednotlivých krocích. Tyto kroky byly identifikace aktiv, identifikace hrozeb s určením jejich vektorů, určení pravděpodobnostního výskytu, zranitelnosti a dopadu. Pro větší přesnost jsem pro výpočet pravděpodobnosti použil optimistický a pesimistický procentní výskyt hrozeb. Z jednotlivých pravděpodobnostních faktorů byla vypočtena konečná hodnota pravděpodobnosti. Zranitelnost a dopad byl spočítán pomocí online kalkulátoru CVSS verze 3.0. Závěrečným krokem bylo stanovení míry rizika a finančního dopadu.

Pro hodnocení rizika jsem si stanovil škálu rizik a matici úrovní rizik pro vzájemné porovnání jednotlivých zařízení. Z vypočtených pravděpodobností a dopadů jsem pomocí uvedené matice stanovil úroveň míry rizika pro jednotlivé hrozby u jednotlivých zařízení. Pro větší přehlednost byly vytvořeny paprskové grafy úrovně rizika.

Lépe z testovaných zařízení dopadla infuzní pumpa, která dosáhla nižších hodnot rizika. Toto zařízení má specifické využití a v současné době není přímo ohroženo kybernetickým útokem. Tři hrozby dosáhly hodnoty 2, tato hodnota znamená zanedbatelné riziko. Čtyři hrozby dosáhly hodnoty 3, toto riziko dosahuje střední hodnoty. Selhání zařízení a neoprávněný přístup dosáhly hodnoty 4. Tato dosažená úroveň nedosahuje kritické hodnoty, přesto je nutno tyto dvě hrozby monitorovat a doporučuji také provést další analýzu rizika v následujícím období. Z hlediska finančního dopadu se na prvním místě s dosaženou největší finanční hodnotou umístila hrozba selhání zařízení a na posledním, tedy devátém místě, se umístila hrozba škodlivý virus. Tyto dosažené hodnoty jsou způsobeny specifičností zařízení.

Zařízení průmyslový robot dosáhl hodnoty míry rizika od 2 do 5. Hrozby sociální inženýrství a hacking dosáhl nejvyšších hodnot. Tato hodnota znamená střední riziko, které je nutné dále monitorovat, aby se riziko ještě nezvýšilo. Hrozba sociální inženýrství dosáhla nejvyšší hodnoty finančního dopadu a naopak nejmenší hodnoty dosáhla hrozba data pocházející z nedůvěryhodných zdrojů. Průmyslový robot je více ohrožen z kyberprostoru a při jeho napadení mohou vzniknout společnosti nemalé škody. Doporučuji takový typ zařízení podrobovat rizikové analýze pravidelně.

Přínos této bakalářské práce je sestavená metodika QRA, která je uplatnitelná nejen pro stanovení samotného rizika, ale také lze porovnat jednotlivé systémy, zařízení či řešení mezi sebou. Výsledky této práce mohou dále posloužit pro vytváření analýz rizika v rámci kybernetické bezpečnosti.

7. Citovaná literatura

[1] Hrůza, Petr. *Kybernetická bezpečnost II.* Brno : Univerzita obrany, 2013. ISBN 978-80-7231-914-5.

[2] Polčák, R., Harašta, J., Stupka, V. *Právní problémy kybernetické bezpečnosti.* Brno : Masarykova univerzita, Právnická fakulta, 2016. Sv. Spisy právnické fakulty MU, řada teoretická, edice Scientia, sv. č. 576. ISBN 978-80-210-8426-1.

[3] Macek, Jakub. Revue pro média č.5. *Kyberprostor.* [Online] 2003. [Citace: 2. prosinec 2018.] http://rpm.fss.muni.cz/Revue/Heslar/kyberprostor.htm.

[4] Jirásek, P., Novák, L., Požár, J. *Výkladový slovník kybernetické bezpečnosti: Cyber Security Glossary.* Praha : Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.

[5] Databáze strategií. *Národní strategie kybernetické bezpečnosti ČR 2015-2020.* [Online] 2. únor 2015. [Citace: 28. duben 2019.] https://www.databaze-strategie.cz/cz/cr/strategie/narodni-strategie-kyberneticke-bezpecnosti-cr-na-obdobi-let-2015-az-2020.

[6] Refsdal, A., Solhaug, B., Stolen, K. *Cyber-Risk Management.* místo neznámé : Springer International Publishing, 2015. ISBN 978-3-319-23569-1.

[7] Beckers, K., Schmidt, H., Kuster, J., Faßbender, S. *Pattern-Based Support for Context Establishment and Asset Identification of the ISO 27000 in the Field of Cloud Computing.* Vídeň : IEEE, 2011. DOI: 10.1109/ARES.2011.55.

[8] Strnád, Ondrej. *Riadenie rizík informačnej bezpečnosti.* Ostrava : AMOS, 2010. ISBN 978-80-904523-9-8.

[9] Stoneburner, G., Goguen, A., Feringa, A. *Risk Management Guide for Information Technology Systems.* Falls Church : National Institute of Standards and Technology, 2002. NIST SP 800-30.

[10] Národní úřad pro kybernetickou a informační bezpečnost. *Co je NCKB.* [Online] 2018. [Citace: 5. prosinec 2018.] https://www.govcert.cz/.

[11] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Sbírka 75/2014 ze dne 29.8.2014.

[12] ASOCIACE za lepší ICT řešení. *Kybernetický bezpečnostní incident.* [Online] 2018. [Citace: 4. říjen 2018.] https://lepsi-reseni.cz/ochrana-osobnich-udaju-gdpr/kyberneticka-bezpecnost-iii-kyberneticky-bezpecnosti-incident/.

[13] KYBEZ. *Řízení bezpečnostních incidentů.* [Online] 2018. [Citace: 4. říjen 2018.] https://www.kybez.cz/bezpecnost/co-delat-kdyz-ochrana-selze.

[14] Hrůza, Petr. *Kybernetická bezpečnost.* Brno : Univerzita obrany, 2012. ISBN 978-80-7231-914-5.

[15] Pandian, C. Ravindranath. *Applied Software Risk Management.* New York : Auerbach Publications, 2007. ISBN 978-0-8493-0524-5.

[16] ČSN ISO/IEC 27005 - Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací 36 9790. ICS 35.040 z července 2013.

[17] Čermák, Miroslav. Clever and Smart. *Analýza rizik: kvantitativní analýza rizik.* [Online] 25. prosinec 2012. [Citace: 6. říjen 2018.] https://www.cleverandsmart.cz/analyza-rizik-kvantitativni-analyza-rizik/.
[18] Roudný, R., Linhart, P. *Krizový management III. Teorie a praxe rizika.* Pardubice : Univerzita Pardubice, 2007. ISBN 80-7194-924-8.
[19] Vose, David. *Risk Analysis - A quantitative guide.* West Sussex : John Wiley & Sons. Ltd., 2008. ISBN 978-0-470-51284-5.
[20] Mulder, Patty. TOOLSHERO. *Heuristic Method.* [Online] 2018. [Citace: 13. prosinec 2018.] https://www.toolshero.com/problem-solving/heuristic-method/.
[21] Probability Formula. *Expected Value.* [Online] 2018. [Citace: 13. prosinec 2018.] http://www.probabilityformula.org/expected-value.html.
[22] Frost, Jim. Statistics By Jim. *Understanding Probability Distributions.* [Online] 2018. [Citace: 13. prosinec 2018.] http://statisticsbyjim.com/basics/probability-distributions/.
[23] Cybenko, G., Hughes, J. TIMREVIEW. *Quantitative Metrics and Risk Assessment.* [Online] srpen 2013. [Citace: 12. prosinec 2018.] https://timreview.ca/sites/default/files/article_PDF/HughesCybenko_TIMReview_August2013.pdf.
[24] ENISA. *Publications.* [Online] European Union Agency for Network and Information Security, 2019. [Citace: 24. únor 2019.] https://www.enisa.europa.eu/.
[25] ENISA. *Cramm.* [Online] European Union Agency for Network and Information Security, 2018. [Citace: 24. únor 2019.] https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_cramm.html.
[26] ENISA. *Mehari.* [Online] European Union Agency for Network and Information Security, 2018/9. [Citace: 24. únor 2019.] https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_mehari.html.
[27] ENISA. *Marion.* [Online] European Union Agency for Network and Information Security, 2017. [Citace: 22. únor 2019.] https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_marion.html.
[28] FIRST. *Common Vulnerability Scoring System SIG.* [Online] 2019. [Citace: 30. duben 2019.] https://www.first.org/cvss/.
[29] WhatIs. *Confidentiality, integrity, and availability (CIA triad).* [Online] 2015. [Citace: 8. květen 2019.] https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA.

[30] Hawkmed. *Shenzhen Hawk Medical Instrument Co., Ltd.* [Online] 2019. [Citace: 8. květen 2019.] https://hawkmed.en.made-in-china.com/.
[31] FANUC. *Průmyslové roboty FANUC.* [Online] 2019. [Citace: 8. květen 2019.] https://www.fanuc.eu/cz/cs/roboty.
[32] FIRST. *Common Vulnerability Scoring System Version 3.0 Calculator.* [Online] 2019. [Citace: 6. květen 2019.] https://www.first.org/cvss/calculator/3.0.
[33] FIRST. *Common Vulnerability Scoring System v3.0: Specification Document.* [Online] [Citace: 7. květen 2019.] https://www.first.org/cvss/specification-document.

Seznam příloh

Příloha 1 - Vzorová tabulka pro výpočet výskytu hrozeb

Označení hrozby			
Popis faktoru	P_{opt}	P_{pes}	**Váha**
Faktor č. 1			
Faktor č. 2			
Faktor č. 3			
Faktor č. 4			
Vážený aritmetický průměr			
Aritmetický průměr			

Příloha 2 - Komentovaný příklad softwaru na výpočet míry rizika

```
System.out.printf("Hrozba (jeji faktory):"); // vypisy hrozeb a jejich faktoru
                System.out.printf("%nVzdalena spionaz (nedostatecne bezpecna sitova architektura, prenos odkrytych hesel, nechranene komunikacni linky, nechranene pripojeni do verejne site)");
                System.out.printf("%nNeduveryhodna data (nekontrolovane stahovani a uzivani programu, nedostatecne zalohovani, nedostatky ve formalnim procesu pro autorizaci verejne pristupnych informaci)");
                System.out.printf("%nSelhani zarizeni (nedostatecne bezpecnostni skoleni, prehrati zarizeni, chyba obsluhy, neopravnene pouziti)");
                System.out.printf("%nChybne fungovani zarizeni (nedostatecna dokumentace, chyba obsluhy, nedostatecne proskolena obsluha, chybny software)");
                System.out.printf("%nZneuziti opravneni (nedostatecne testovani programu, zname chyby v programech, neodhlaseni se pri opousteni pracovni stanice)");
                System.out.printf("%nSocialni inzenyrstvi (phishing, baiting, sniffing, malware)");
                System.out.printf("%nHacking (nedostatecne silna hesla, slabina v systemu, nekontrolovane kopirovani)");
                System.out.printf("%nSkodlivy virus (zneuziti opravneni, nedostatecne silna hesla, nekontrolovane stahovani a uzivani programu, nedostatek kontrolnich mechanizmu)");
                System.out.printf("%nNeopravneny pristup do systemu (nedostatecne silna hesla, neumyslne chyby a opomenuti, chybne prirazeni pristupovych prav, neodhlaseni se pri opousteni pracovni stanice)");

                System.out.printf("%n%nZadejte 4 pravdepodobnosti optimistickeho scenare v intervalu 0-1 (pokud 4. pravdepodobnost neexistuje, pouzijte nulu):"); // zadavani hodnot pro vypocet optimistickeho scenare
                double opt1 = scanner.nextDouble();
                double opt2 = scanner.nextDouble();
                double opt3 = scanner.nextDouble();
                double opt4 = scanner.nextDouble();
                System.out.println("Zadejte 4 pravdepodobnosti pesimistickeho scenare v intervalu 0-1 (pokud 4. pravdepodobnost neexistuje, pouzijte nulu):"); // zadavani hodnot pro vypocet pesimistickeho scenare
                double pes1 = scanner.nextDouble();
                double pes2 = scanner.nextDouble();
                double pes3 = scanner.nextDouble();
                double pes4 = scanner.nextDouble();
                System.out.println("Zadejte 4 vahy scenaru v intervalu 0-1 (pokud nemate 4. pravdepodobnost, pouzijte nulu):"); // zadavani vah scenaru
                double vaha1 = scanner.nextDouble();
                double vaha2 = scanner.nextDouble();
                double vaha3 = scanner.nextDouble();
                double vaha4 = scanner.nextDouble();

                double vazenyPrumer1 = ((opt1 * vaha1) + (opt2 * vaha2) + (opt3 * vaha3) + (opt4 * vaha4))/(vaha1 + vaha2 + vaha3 + vaha4); // vypocet vazeneho prumeru optimistickeho scenare
                double vazenyPrumer2 = ((pes1 * vaha1) + (pes2 * vaha2) + (pes3 * vaha3) + (pes4 * vaha4))/(vaha1 + vaha2 + vaha3 + vaha4); // vypocet vazeneho prumeru pesimistickeho scenare
                System.out.println("Vysledny vazeny prumer u optimistickeho scenare je: " + vazenyPrumer1); // vypis hodnoty optimistickeho scenare
                System.out.println("Vysledny vazeny prumer u pesimistickeho scenare je: " + vazenyPrumer2); // vypis hodnoty pesimistickeho scenare
                System.out.println("Vysledny aritmeticky prumer obou scenaru je: " + (vazenyPrumer1 + vazenyPrumer2)/2); // vypis hodnoty aritmetickeho prumeru

                double aritmetickyPrumer = (vazenyPrumer1 + vazenyPrumer2)/2;

                System.out.println("Zadejte miru dopadu v intervalu 0-10:"); // zadavani miry dopadu
                double dopad = scanner.nextDouble();

                System.out.println("Vysledna mira rizika je: " + aritmetickyPrumer * dopad); // vypis hodnoty vysledne miry rizika
```